AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 18

112TH CONGRESS
1st Session

SENATE

REPORT
112–13

THE USA PATRIOT ACT SUNSET EXTENSION ACT OF 2011

APRIL 5, 2011.—Ordered to be printed

Mr. LEAHY, from the Committee on the Judiciary, submitted the following

R E P O R T

together with

MINORITY VIEWS

[To accompany S. 193]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to which was referred the bill (S. 193), to extend the sunset of certain provisions of the USA PATRIOT Act and the authority to issue national security letters, and for other purposes, having considered the same, reports favorably thereon, with amendments, and recommends that the bill, as amended, do pass.

CONTENTS

		Page
I.	Background and Purpose of The USA PATRIOT Act Sunset Extension Act of 2011	2
II.	History of the Bill and Committee Consideration	20
III.	Section-by-Section Summary of the Bill	22
IV.	Congressional Budget Office Cost Estimate	27
V.	Regulatory Impact Evaluation	31
VI.	Conclusion	31
VII.	Minority Views	32
VIII.	Changes to Existing Law Made by the Bill, as Reported	52

99–010

I. BACKGROUND AND PURPOSE OF THE USA PATRIOT ACT SUNSET EXTENSION ACT OF 2011

A. INTRODUCTION

In the immediate aftermath of the September 11, 2001 attacks, Congress drafted legislation to provide law enforcement with new or expanded tools to investigate and prosecute terrorists. The Senate passed a bill, the Uniting and Strengthening America Act on October 11, 2001. The House passed a bill on October 12, 2001, titled the Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act. The bills were reconciled, producing the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, which was signed into law on October 26, 2001, as P.L. 107–056.

The USA PATRIOT Act triggered significant debate over the scope and targets of its surveillance authorities and the level of judicial review to be applied to the new law. Then-Majority Leader of the House, Richard Armey, and Chairman of the Senate Judiciary Committee, Patrick Leahy, insisted that a four-year sunset apply to 16 authorities. Modifications to National Security Letter (NSL) authorities were enacted without significant controversy in 2001, but subsequent misuse and abuse of NSLs led to intensive public scrutiny and congressional oversight.

The four-year sunsets in the 2001 law would have resulted in the expiration of 16 provisions on December 31, 2005. In enacting a reauthorization law, Congress determined that 14 of the 16 could be made permanent. However, a great deal of controversy continued to surround two authorities: requests for business records (section 215 of the 2001 law), and the "roving" intelligence wiretap authority (section 206 of the 2001 law). In addition, NSLs were closely examined as their use expanded exponentially.

Following intensive debate of the USA PATRIOT Act Improvement and Reauthorization Act of 2005 ("2005 USA PATRIOT Act Reauthorization") conference report, civil liberties concerns led to a bipartisan Senate filibuster of the conference report in December 2005. Congress passed a short extension, finally enacting the conference report and an improvements bill in March 2006 (P.L. 109–177 and P.L. 109–178). Sections 206 and 215 of the 2001 law were subject to a new sunset of December 31, 2009. A third sunset on the same date was imposed on the "lone wolf" surveillance authority, first enacted in 2004 as part of the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108–458). The 2005 USA PATRIOT Act Reauthorization required that audits of section 215 orders and NSLs be conducted by the Inspector General of the Department of Justice. The Inspector General found a small number of instances of improper use of section 215 orders that resulted in the over-collection of information by the FBI. The NSL audits, published in 2007 and 2008, documented wide misuse and some abuse of the NSL authority by the FBI, including improper issuance of so-called "exigent letters."

During the 111th Congress, Chairman Leahy introduced the USA PATRIOT Act Sunset Extension Act of 2009 (S. 1692), which extended the sunsets of the three expiring PATRIOT Act provisions from December 31, 2009 to December 31, 2013. The bill also in-

cluded a number of improvements and reforms that enhanced judicial and congressional oversight, and strengthened important privacy and civil liberties protections. Although S. 1692 was reported out of the Judiciary Committee with bipartisan support,[1] the full Senate did not take further action on the legislation. Instead, two successive short-term extensions of the expiring PATRIOT Act provisions were enacted, ultimately extending the sunset date to February 28, 2011. Another short-term extension enacted in the 112th Congress extended that sunset to May 27, 2011.

The USA PATRIOT Act Sunset Extension Act of 2011 (S. 193) is virtually identical to the bill reported by Chairman Leahy in the 111th Congress (S. 1692). As was the case with S. 1692, the USA PATRIOT Act Sunset Extension Act of 2011 (S. 193) is the product of extensive bipartisan negotiations with the Department of Justice and the intelligence community, and received bipartisan support in Committee.[2]

B. PRIOR CONSIDERATION OF USA PATRIOT ACT AUTHORITIES

During the 109th Congress, a number of the expiring provisions of the 2001 USA PATRIOT Act were considered for reauthorization. The majority of the provisions subject to a sunset were made permanent. However, many Senators including a number on the Senate Committee on the Judiciary expressed continuing concerns with the broad scope of information-gathering powers afforded the Government. These Senators sought additional protections against possible infringements on the constitutional rights and civil liberties of U.S. persons. In particular, concerns were raised about sections 206 and 215 of the 2001 USA PATRIOT Act, which authorized "roving" wiretaps and orders for production of business records under the Foreign Intelligence Surveillance Act of 1978 ("FISA"). The "lone wolf" surveillance authority, which had been included in FISA through the Intelligence Reform and Terrorist Prevention Act of 2004, was also viewed as controversial by some. Accordingly, the 2005 USA PATRIOT Act Reauthorization included a new sunset of December 31, 2009, for these three provisions. The 2005 USA PATRIOT Act Reauthorization also mandated that the Department of Justice, Office of Inspector General complete comprehensive audits on the Government's use of NSLs and requests for production of business records and other tangible things under section 215 of the 2001 USA PATRIOT Act.

The sunset and auditing measures required by that law proved that continuing congressional oversight and procedural protections are vital to ensuring that the Government's powers are exercised in a manner that is consistent with the constitutional rights and civil liberties of Americans. In 2007 and 2008, the Department of Justice, Office of Inspector General issued reports on the use of NSLs and requests for section 215 orders for business records by the Federal Bureau of Investigation (FBI), and found numerous instances of over-collection of information. In reports on the use of NSLs, the Inspector General cited faulty record keeping, poor

[1] Among the Republican members of the Committee, both Senator Kyl and Senator Cornyn supported S. 1692 and voted to report the bill favorably to the full Senate.

[2] During consideration of the bill in the 112th Congress, among the Republican members of the Committee, Senator Lee supported S. 193 and voted to report the bill favorably to the full Senate.

tracking systems, and both misuse and abuse of the NSL authority. For example, a March 2007 report by the Department of Justice Inspector General "concluded that the FBI engaged in serious misuse of NSL authority," including improper authorization of NSLs, improper requests under the pertinent national security letter statutes, and unauthorized collections. (Report of the U.S. Department of Justice, Office of the Inspector General, "A Review of the Federal Bureau of Investigation's Use of National Security Letters, March 2007," found at *http://www.justice.gov/oig/special/s0703b/final.pdf*.)

Most troubling, the report also identified more than 700 instances in which the FBI improperly obtained telephone records by issuing "exigent letters." (Id. p. 86–97) The Department of Justice Inspector General also found instances in which improper use of section 215 orders for business records or other tangible things by the FBI resulted in over-collection of information, or where the FBI issued NSLs to obtain information for which the Foreign Intelligence Surveillance Court ("FISA Court") had previously refused to authorize a section 215 order, based on First Amendment concerns. (Report of the U.S. Department of Justice, Office of the Inspector General, "A Review of the FBI's Use of Section 215 Orders for Business Records in 2006," March 2008, at pp. 59–74; found at *http://www.justice.gov/oig/special/s0803a/final.pdf*.)

Consistent with the 2005 USA PATRIOT Act Reauthorization, S. 193, the USA PATRIOT Act Sunset Act of 2011, mandates further audits to ensure that these surveillance authorities are implemented properly. It also adds a new set of audits to review the use of pen register and trap and trace devices authorized under FISA.

Early in the 111th Congress, with a December 31, 2009, sunset pending, Chairman Leahy wrote to Attorney General Eric Holder seeking the administration's views on reauthorization of the expiring authorities. (Letter from Chairman Leahy to Attorney General Eric Holder, dated March 9, 2009.) The Assistant Attorney General for Legislative Affairs, Ronald Weich, responded to Chairman Leahy on September 14, 2009, stating that the Department of Justice would prefer to have the authorities extended, and that the Department of Justice would be willing to work with the Committee to consider additional privacy protections for law abiding Americans. (Letter from Assistant Attorney General for Legislative Affairs, Ronald Weich, to Chairman Leahy, dated September, 14, 2009.)

The Committee held a hearing titled, "Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security," on September 23, 2009. (See Hearing of the Senate Committee on the Judiciary, "Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security," September 23, 2009, S. Hrg. 111–333, Serial No. J–111–49, available at *http://www.gpo.gov/fdsys/pkg/CHRG-111shrg55610/pdf/CHRG-111shrg55610.pdf*.) During the first panel, testimony was heard from David Kris, Assistant Attorney General for the National Security Division of the Department of Justice and Glenn Fine, the Inspector General of the Department of Justice.

Mr. Kris requested that the three expiring provisions of the USA PATRIOT Act be reauthorized. The three provisions, which were then set to expire on December 31, 2009, are the FISA "roving" wiretap authority, the "lone wolf" surveillance authority, and the

provision authorizing FISA orders for business records and other tangible things. (Id. at 107–112.)

Mr. Fine summarized the findings of audits conducted by the Office of the Inspector General on the use of NSLs and orders for business records. These audits were required by sections 119 and 106A of the 2005 USA PATRIOT Act Reauthorization. (Id. at 81–96.) As noted above, the audits found significant problems regarding the use of NSLs and exigent letters.

During the second panel, testimony was received from three experts in national security law. Suzanne Spaulding, principal of the Bingham Consulting Group, testified in favor of reforms to the three expiring provisions of the USA PATRIOT Act. Kenneth Wainstein, a partner at O'Melveny & Myers, stated that the expiring provisions contained adequate safeguards and should be reauthorized. Lisa Graves, executive director of the Center for Media & Democracy, critiqued the use of orders for business records and NSLs and recommended that higher standards for issuance of such orders be enacted. The full hearing record is available at *http://www.gpo.gov/fdsys/pkg/CHRG-111shrg55610/pdf/CHRG-111shrg55610.pdf*.)

In the 111th Congress, the Committee reported the USA PATRIOT Act Sunset Extension Act of 2009, S. 1692. That bill, reported on October 13, 2009, received a bipartisan vote in the Committee, with Senators Kyl (R–AZ) and Cornyn (R–TX) voting in favor of the bill, along with Chairman Leahy (D–VT) and Senators Kohl (D–WI), Feinstein (D–CA), Schumer (D–NY), Cardin (D–MD), Whitehouse (D–RI), Klobuchar (D–MN), Kaufman (D–DE), and Franken (D–MN). After the bill was reported, Senators Kyl and Sessions (R–AL) joined with Chairman Leahy, Senator Feinstein, the Department of Justice, and intelligence agencies to continue negotiations over the legislative text. In November 2009, the revised bill text was finalized. The bill was endorsed by the Attorney General in a letter to Chairman Leahy dated November 9, 2009. The bill was again endorsed by the Attorney General and the Director of National Intelligence in a letter to the Leaders of the House of Representatives and the Senate dated February 19, 2010.

Instead of taking further action on S. 1692 in the 111th Congress, two short-term extensions of the expiring provisions of the USA PATRIOT Act were enacted, ultimately extending the sunset date to February 28, 2011.

On March 17, 2010, following enactment of the February 28, 2011 sunset extension, Chairman Leahy wrote to the Attorney General, asking him to implement a number of the provisions of the negotiated package based on S. 1692, which the administration had strongly endorsed. Chairman Leahy noted in his letter that the majority of provisions in the package did not require legislative action, but could be implemented as a matter of administrative policy and practice. The Attorney General responded to Chairman Leahy's letter on December 9, 2010. The Attorney General agreed to implement a significant number of the provisions, and stated: "[W]e have determined that many of the privacy and civil liberties provisions of S. 1692 can be implemented without legislation." He continued: "We believe these measures will enhance standards, oversight, and accountability, especially with respect to how information about U.S. persons is retained and disseminated, without sacrificing the

operational effectiveness and flexibility needed to protect our citizens from terrorism and facilitate the collection of vital foreign intelligence and counterintelligence information.'' (Letter from Attorney General Eric Holder to Chairman Leahy dated December 9, 2010.)

In his response to Chairman Leahy's request, the Attorney General specifically outlined a number of provisions that the Department of Justice could implement administratively without impacting operational ability to protect Americans from terrorism. For example, regarding section 215 orders for tangible things, the Attorney General agreed to apply new requirements for acquisition of library and bookseller records. Specifically, when library or bookseller records are sought using a section 215 order, the Government must provide a statement of facts showing reasonable grounds to believe the tangible things are relevant to an authorized investigation and pertain to (a) an agent of a foreign power, (b) the activities of a suspected agent, or (c) an individual in contact with or known to a suspected agent of a foreign power subject to the investigation.

With regard to NSLs, to facilitate better auditing and accountability, the Department of Justice adopted a policy requiring the FBI to retain a written statement of facts showing that the information sought through an NSL is relevant to an authorized investigation. In addition, the Department of Justice adopted procedures to provide notification to recipients of NSLs of their opportunity to contest any nondisclosure requirement attached to the NSL. The Department of Justice further agreed to ensure that NSL recipients who challenge nondisclosure orders are notified by the FBI when compliance with such nondisclosure orders is no longer required.

The bill in the 111th Congress (S. 1692) called upon the Department of Justice to adopt procedures for the collection, use, and storage of information derived from NSLs. Those procedures were approved by Attorney General Holder on October 1, 2010. Finally, the Attorney General agreed to work with Congress to determine ways to make additional information regarding the use of FISA authorities publicly available.

Chairman Leahy also wrote to Justice Department Inspector General Glenn Fine on March 16, 2010, requesting that the Office of the Inspector General fulfill several auditing and reporting requirements included in the legislation. On June 15, 2010, Inspector General Fine responded, indicating that his office would conduct many of the audits called for in the legislation. (Letter from Department of Justice Inspector General Glenn Fine to Chairman Leahy dated June 15, 2010.)

C. CONSIDERATION OF USA PATRIOT ACT AUTHORITIES IN THE 112TH CONGRESS

Early in the 112th Congress, facing a sunset date of February 28, 2011, Congress enacted a short-term extension of the three expiring provisions of the USA PATRIOT Act to May 27, 2011.

The USA PATRIOT Act Sunset Extension Act of 2011, S. 193 as introduced, was virtually identical to the version of S. 1692 that was negotiated in the 111th Congress with Senators Kyl (R–AZ), Sessions (R–AL), Leahy (D–VT), and Feinstein (D–CA), along with the Department of Justice, and intelligence agencies. The only differences between the negotiated package of November 2009 and S.

193 as introduced are updates to the dates by which Inspectors General must submit audits to Congress. In addition, the new bill contains a modification to reflect that procedures for the collection, use and storage of information derived from NSLs were established by the Department of Justice in October 2010. Rather than calling for the establishment of such procedures, the new bill requires the Attorney General to periodically review the procedures, taking the privacy rights and civil liberties of Americans into consideration.

With those slight modifications, the text of S. 193 as introduced is substantively identical to the package that the Department of Justice and Office of the Director of National Intelligence (DNI) have repeatedly endorsed and have stated will pose no operational concerns for law enforcement or intelligence collection. Indeed, in light of the commitments by the Attorney General and the Inspector General for the Department of Justice to implement administratively a number of the provisions of S. 1692 (111th Congress), S. 193 simply codifies much of what the administration is already doing. The administration confirmed in a February 28, 2011, briefing for Senators that the prior endorsement letters of November 9, 2009, and February 19, 2010, remain in force.

On February 8, 2011, the Chairman and Vice Chairman of the Senate Select Committee on Intelligence wrote to each Member of the Senate that the Attorney General and the Director of National Intelligence had provided a classified report for review by all Senators in connection with the sunset of FISA authorities. The letter invited each Senator to read the classified report at the Senate Intelligence Committee. The letter also advised that the Attorney General and the DNI had offered to make Justice Department and Intelligence Community personnel available to meet with any Member who has questions.

On February 14, 2011, the Director of the FBI, Robert Mueller; the Director of National Intelligence, James Clapper; and the Director of the National Security Agency, General Keith Alexander, briefed members of the Senate Judiciary and Intelligence Committees. A classified briefing was held on February 28, 2011, for the same group of Senators, with the Assistant Attorney General for National Security, David Kris; General Counsel of the FBI, Valerie Caproni; General Counsel to the Director of National Intelligence, Robert Litt; and General Counsel of the National Security Agency, Matthew Olsen. The briefers reiterated that S. 193 poses no operational concerns and is the product of extensive negotiations between the Executive Branch and Congress in 2009.

On March 1, 2011, in testimony before the House Appropriations Subcommittee on Commerce, Justice, and Science, Attorney General Holder stated his support for S. 193, saying that the bill strikes "a good balance," in that it extends authorities subject to sunset, "but also dials in civil liberties protections." In addition, in hearing testimony before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security, on March 9, 2011, the Acting Assistant Attorney General for National Security, Todd Hinnen, said: "The administration had reached the point where it was supporting a very similar bill to [S. 193] at the end of the last Congress . . . [W]e are prepared to support a bill that's similar to the one that was at the close of the last Congress." Mr. Hinnen also confirmed that the FISA "lone wolf" provision has still

never been used by the Government. In the same hearing, the General Counsel to the Director of National Intelligence, Robert Litt, said: "I think the provisions in [S. 193] are examples of the kinds of provisions that I described in my statement as provisions that would provide enhanced protection for civil liberties without affecting operational utility."

The USA PATRIOT Act Sunset Extension Act of 2011, S. 193, as amended and reported by the Committee, and as described more fully below, recognizes the Government's need to maintain the tools necessary for effective counterterrorism investigations while protecting the civil liberties and constitutional rights so important to all Americans. The bill extends to December 31, 2013 the sunset on the three expiring provisions: "roving" wiretaps, section 215 orders for business records and tangible things, and the "lone wolf" provision. It also imposes a new sunset on the use of NSLs.

In expressing support for periodic review and oversight, a number of former intelligence officials and national security experts wrote to Senate Leadership on February 9, 2011, that: "A permanent extension . . . risks avoiding the kind of assessment of authorities for national security investigations that we believe is required to ensure that they adequately and appropriately preserve civil liberty and privacy and protect national security." (Letter from William Banks, Director of the Institute for National Security and Counterterrorism at Syracuse University College of Law, et al, to Senators Reid and McConnell, dated February 9, 2011.)

A September 14, 2009, letter to this Committee from the Department of Justice acknowledged that: "The oversight provided since 2001 and the specific oversight provisions that were added to the statute in 2006 have helped to ensure the authority is being used as intended." The bill as reported expands oversight by mandating new audits by the Inspector General of the Department of Justice, requiring new court-approved minimization procedures on surveillance authorities, and including more detailed public reporting on the use of surveillance under FISA. As set forth more fully below, the bill strengthens oversight and judicial review, and addresses constitutional concerns about NSL nondisclosure orders raised by the United States Court of Appeals for the Second Circuit. See *Doe* v. *Mukasey*, 549 F.3d 861 (2d Cir. 2008).

The bill has been endorsed by the Fraternal Order of Police, which stated that the "bill will maintain tools used by law enforcement . . . without additional barriers or legal loopholes." (Letter from Chuck Canterbury, National President, National Fraternal Order of Policy, to Chairman Leahy, Dated March 14, 2011.) In addition, S. 193 was endorsed by the Vermont Library Association, the American Library Association, the Association of Research Libraries, the American Association of Law Libraries, the Medical Library Association, and the Special Library Association.

D. EXPIRING PROVISIONS OF THE USA PATRIOT ACT

1. Section 215 Orders for Tangible Things

Section 215 of the 2001 USA PATRIOT Act (codified at 50 U.S.C. § 1861) amended FISA to enable the Government to apply for an order requiring an individual or entity to produce tangible things—including books, records, papers, or documents—that are relevant

to an authorized investigation involving foreign intelligence, international terrorism, or clandestine intelligence activities. Since its passage in 2001, this provision of the USA PATRIOT Act—sometimes called the "library provision" because of concerns that the Government could use it to obtain records and patron lists from libraries and bookstores—has been extremely controversial. It expires on May 27, 2011.

a. History and Current Law on Section 215 Orders for Business Records and Other Tangible Things

As originally enacted, FISA did not contain any provision authorizing the Government to require the production of documents or tangible things. In 1998, Congress amended FISA to allow the FBI to apply for a court order to obtain "records" from a "common carrier, public accommodation facility, physical storage facility, or vehicle rental facility." From 1998–2001, any records sought under this provision had to be for "an investigation to gather foreign intelligence information or an investigation concerning international terrorism," and the application had to provide "specific and articulable facts giving reason to believe that the person to whom the records pertain [was] a foreign power or an agent of a foreign power."

The 2001 USA PATRIOT Act eliminated the restriction on the types of entities that were subject to this authority. Current law enables the FBI to seek production from any person or entity. The 2001 USA PATRIOT Act also expanded the scope of this authority by allowing the Government to seek "any tangible things"—not just "records".

Additionally, the 2001 USA PATRIOT Act and the subsequent 2005 USA PATRIOT Act Reauthorization lowered the standard for obtaining section 215 orders by eliminating the requirement that an application specify "specific and articulable facts" giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power. Under current law, the records or tangible things sought need not pertain to a foreign power or an agent of a foreign power. Instead, a statement of facts demonstrating mere relevance to an authorized investigation is sufficient.

Under current law, in order to obtain a section 215 order, the Government must submit a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation to: (1) obtain foreign intelligence information (not concerning a United States person); (2) protect against international terrorism; or (3) protect against clandestine intelligence activities. The underlying investigation must be conducted in accordance with Attorney General guidelines, and may not be conducted on a U.S. person based solely on that person's First Amendment activity.

Tangible things are presumptively relevant to an investigation if they pertain to any of the following: (1) a foreign power or an agent of a foreign power; (2) the activities of a suspected agent of a foreign power who is the subject of an authorized investigation; or (3) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of an authorized investigation. When the FBI seeks production of certain materials, including li-

brary circulation records, library patron lists, book sales records, firearms sales records, tax return records, educational records, or medical records, the application can be made by only a handful of high-ranking FBI officials. In all other instances, the authority to apply for section 215 orders can be delegated to the heads of FBI field offices. A recipient of a section 215 production order may challenge the legality of that order by filing a petition with the FISA Court.

A recipient of a section 215 order may not disclose that fact, except to those persons to whom disclosure is necessary to comply with the order, or to an attorney to obtain legal advice or assistance with respect to the production of things in response to the order. The recipient may challenge these nondisclosure requirements—but only after a year has passed since receipt of the section 215 order. The court must apply a conclusive presumption that nondisclosure is justified if the Government certifies that it would endanger national security.

b. Changes to Section 215 Contained in S. 193, as Reported

The USA PATRIOT Act Sunset Extension Act of 2011 adjusts the requirements for obtaining a court order for tangible things under FISA. First, the language modifies the statute slightly to strike the requirement for a "statement of facts," and instead requires "a statement of the facts and circumstances relied upon by the applicant to justify the belief of the applicant" that the items sought are relevant to an authorized investigation. The language in the bill does not raise the standard, and is not intended to affect or restrict any activities approved by the FISA Court under existing statutory authorities. In addition, it is not vague or untested language. In fact, other sections of FISA use identical language. These are section 104 of FISA, which governs electronic surveillance, and section 303 of FISA, which covers physical searches.

Second, the bill removes the presumption of relevance described above. The bill requires the Government to provide a statement of the facts and circumstances relied upon by the applicant to justify the applicant's belief that the tangible things sought are relevant. The Department of Justice has indicated that it does not rely on this presumption, and that its current practice is to provide the Foreign Intelligence Surveillance Court with a complete statement of facts to support issuance of an order.

Third, to obtain library records that contain personally identifiable information about a library patron, or bookseller records, the bill requires the Government to provide a statement of facts showing reasonable grounds to believe the tangible things are relevant to an authorized investigation and pertain to (a) an agent of a foreign power, (b) the activities of a suspected agent, or (c) an individual in contact with or known to a suspected agent of a foreign power subject to the investigation. "Bookseller records" are defined as meaning any transactional records reflecting the purchase or rental of books, journals, or magazines, whether in digital or print form. In a letter to Chairman Leahy dated December 9, 2010, the Attorney General agreed to implement this library and bookseller records requirement administratively. (Letter from Attorney General Eric Holder to Chairman Leahy dated December 9, 2010.)

Fourth, the bill repeals the one-year waiting period for the recipient of a section 215 order to be able to challenge an accompanying nondisclosure or "gag" order. It also repeals a provision added to the law in 2006 stating that a conclusive presumption in favor of the Government shall apply where a high level official certifies that disclosure of the order for tangible things would endanger national security or interfere with diplomatic relations. The Department of Justice has stated that it has no objection to repealing these provisions.

2. "Roving" Wiretaps

a. History and Current Law on "Roving" Wiretaps

Section 206 of the 2001 USA PATRIOT Act expanded the wiretap provisions of FISA to permit the Government to obtain secret "roving" wiretap orders in intelligence investigations.

Previously, a wiretap order under FISA had to identify both the person who is the target of the surveillance and the phone or computer to be wiretapped. Section 206 authorized the FISA Court to issue wiretap orders that identify the target of the surveillance but not the specific communications device being used by the target—effectively permitting the Government to wiretap new phones or computers being used by that target without going back to the court for advance approval.

To obtain a "roving" wiretap order under FISA, the Government must demonstrate to the court that the actions of the target may have the effect of thwarting surveillance. In addition, changes made during the 2005 USA PATRIOT Act Reauthorization process require the Government to report to the FISA Court whenever it initiates surveillance on a new phone or computer not listed in the original "roving" wiretap order.

The criminal wiretap law permits "roving" wiretaps, as well, but it contains additional safeguards that the FISA "roving" wiretap provision does not. First, FISA permits a "John Doe roving wiretap" that does not identify the person or the phone to be wiretapped. The criminal law contains no such provision. Second, the criminal wiretap law permits surveillance of a new phone or computer under a "roving" wiretap order only while agents have some indication the target is using it. Specifically, under the criminal law, surveillance is allowed "only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted." This is often called the "ascertainment" requirement, and FISA does not contain such a requirement for FISA "roving" wiretaps.

b. Changes made to the Wiretap Statute Contained in S. 193, as Reported

In addition to placing a new sunset on the FISA "roving" wiretap authority of December 31, 2013, the bill modifies the requirement for FISA wiretap orders. This section is intended to amend the FISA wiretap statute (50 U.S.C. 1805(c)(1)(A)) so as to require law enforcement to identify "with particularity" the target of a wiretap request under FISA. The Department of Justice has testified that, in applications to the FISA Court for "roving" wiretaps, it already,

as a matter of practice, provides the court sufficient detail to identify the target with particularity. (Written Testimony of Acting Assistant Attorney General Todd Hinnen, Department of Justice, National Security Division, before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security, March 9, 2011, at p. 2).

3. "Lone Wolf" Surveillance Authority

a. History of the "Lone Wolf" Surveillance Authority

The Intelligence Reform and Terrorism Prevention Act of 2004 included a provision that created a new category of persons subject to surveillance under FISA, titled "Individual Terrorists as Agents of Foreign Powers." (P.L. 108–458, Sec. 6001.) This provision is often called the "lone wolf" provision. It expires on May 27, 2011.

Under FISA, a "lone wolf" is a person the Government has probable cause to show is engaging or preparing to engage in "international terrorism," and who is not a U.S. person, meaning not a U.S. citizen or a lawful permanent resident. This definition may include a person who has no known ties to a foreign organization or government. Prior to enactment of this section, FISA required such a foreign nexus.

"Lone wolf" is often called the "Moussaoui fix," but that label is a misnomer. The misunderstanding stems from claims that the FBI was unable to search a computer used by Zacharias Moussaoui, the so-called 20th hijacker in the September 11, 2001, attacks, because it could not establish probable cause to believe he was acting on behalf of a foreign power. Those claims are inaccurate, however, and the FBI later admitted in testimony before Congress that the agent in charge of the investigation did not understand that probable cause was the standard, what probable cause meant in this context, or the legal definition of an agent of a foreign power.[3]

b. Changes made to the "Lone Wolf" Statute Contained in S. 193, as Reported

The bill makes no changes to the "lone wolf" statute; it merely ensures continuing congressional oversight by extending the sunset from May 27, 2011, to December 31, 2013.

E. OTHER SURVEILLANCE PROVISIONS OF THE USA PATRIOT ACT ADDRESSED IN S. 193

1. National Security Letter (NSL) Authority

a. History of NSL Authority

A National Security Letter (NSL) is a surveillance tool that allows intelligence and law enforcement officials to obtain certain types of communications and financial records sought in connection with intelligence and national security investigations.

---

[3] The suggestion in the Minority Views that the "lone wolf" provision "ha[s] helped federal law enforcement and intelligence agencies stay ahead of terrorists to prevent or thwart planned attacks" is inaccurate. During testimony before the Committee on March 30, 2011, FBI Director Robert Mueller confirmed that the "lone wolf" authority has still never been used. Accordingly, it is similarly inaccurate and illogical to suggest that the "lone wolf" authority should be made permanent because it has never been abused. To the contrary, significant questions have been raised about the constitutionality of wiretapping a person in the U.S. who has committed no crime and has no connection to international terrorist organizations, as the "lone wolf" provision allows.

National Security Letters were first authorized by the Right to Financial Privacy Act (RFPA) in 1986. By 2001, there were four NSL authorities in place under the RFPA, the Electronic Communications Privacy Act, the Fair Credit Reporting Act, and the National Security Act. The 2001 USA PATRIOT Act added a fifth NSL authority under the Fair Credit Reporting Act. Before 2001, NSLs allowed the FBI limited access to financial, credit agency, telephone, Internet Service Provider, and other communications records.

Under current law, the Government can obtain such records if the information sought is relevant to an investigation to protect against international terrorism or espionage. The Government does not need to show that the records sought pertain to or are otherwise connected to a foreign power or an agent of a foreign power.

National Security Letters do not require a court order. They are a form of administrative subpoena issued by FBI and other officials. Typically, they are served with nondisclosure orders, or "gag" orders, prohibiting the recipient from revealing its issuance.

b. Expansion of NSL Authority Under the 2001 USA PATRIOT Act

Prior to 2001, an FBI official had to show a factual basis for believing that the records sought pertained to an agent of a foreign power before issuing an NSL.

Section 505 of the 2001 USA PATRIOT Act expanded the NSL authorities in ways not contemplated by the original RFPA in 1986. The result of these changes is that the FBI may now obtain information on individuals who are not the subjects of national security investigations. It eliminated the requirement that the information sought pertain to a foreign power or an agent of a foreign power. It also eliminated the requirement to show a factual basis, enabling the FBI to rely upon mere relevance to an investigation to protect against international terrorism or foreign espionage.

The 2001 USA PATRIOT Act also expanded the authority to issue NSLs beyond FBI headquarters to include the heads of the FBI field offices (i.e., Special Agents in Charge). The 2001 USA PATRIOT Act also expanded the list of authorized issuers of certain NSLs under the Fair Credit Reporting Act to include intelligence agencies.

c. Further Expansions of NSL Authority Enacted in 2004

The Intelligence Authorization Act for FY 2004 (P.L. 108–177) modified the definition of "financial institution" to allow the FBI to issue NSLs under the Right to Financial Privacy Act to a much broader range of businesses, including travel and real estate agencies, jewelers, insurance companies, casinos, car dealers, and the U.S. Postal Service. Financial records were redefined to include "any record held by a financial institution pertaining to a customer's relationship with the financial institution."

The FBI issued policy guidance in 2007 stating that FBI officials should not rely upon this statute to obtain records from the expanded list above that were not "financial in nature."

d. The 2005 USA PATRIOT Act Reauthorization Governs Challenges to NSLs

The 2005 USA PATRIOT Act Reauthorization addressed how the Government may compel compliance with both an NSL and a nondisclosure order accompanying an NSL.

The law gave the Government explicit power to compel compliance with an NSL. Failure to comply may be punished with contempt of court. If the recipient of a nondisclosure order knowingly and with intent to obstruct an investigation discloses its existence, the recipient faces five years in prison.

The law allows the recipient of a nondisclosure order to challenge the nondisclosure in Federal court. If the challenge is filed within a year of issuance, however, and the Government certifies that disclosure may harm national security, the judge must treat that certification as conclusive. If the recipient challenges the nondisclosure after one year, the Government must recertify harm to national security or terminate the nondisclosure order. The 2005 USA PATRIOT Act Reauthorization also gave the recipient of an NSL the ability to challenge it in Federal District Court. In 2008, the United States Court of Appeals for the Second Circuit found the NSL nondisclosure provisions unconstitutional. *Doe* v. *Mukasey*, 549 F.3d 861 (2d Cir. 2008). The USA PATRIOT Act Sunset Extension Act of 2011, S. 193, codifies the process suggested by the Second Circuit to correct this constitutional defect (see below). Without this legislative correction, the nondisclosure provision remains constitutionally infirm.

e. Changes to NSL Authority Contained in S. 193, as Reported

The USA PATRIOT Act Sunset Extension Act of 2011, S. 193, does not raise the standard for issuing an NSL but does make some targeted changes to ensure NSLs are issued in full compliance with law and practice.

The instances of FBI misuse and abuse of NSLs discussed above are well documented. Therefore, to ensure that NSLs are not being issued arbitrarily, the bill requires the FBI to retain a written statement of specific facts demonstrating the relevance of the NSL to an authorized investigation. This allows FBI supervisors to ensure that agents are using NSLs properly, and provides auditors with the information necessary to audit NSL records.

The Attorney General has stated that retention of a written statement of facts is exactly what current FBI policy requires. The new computer system requires the FBI to add the statement of facts to the application for an NSL. Therefore, the bill would simply codify current FBI practice. There would be no new recordkeeping requirements imposed on the FBI.

Second, the bill corrects the constitutional defects in the issuance of nondisclosure orders on NSLs as found by the United States Court of Appeals for the Second Circuit in *Doe* v. *Mukasey*, 549 F.3d 861 (2d Cir. 2008), and adopts the concepts suggested by that court for a constitutionally sound process. Id. at 883–84. The bill allows the recipient of an NSL with a nondisclosure order to notify the Government at any time that it wishes to challenge the nondisclosure order. The Government then has 30 days to seek a court order in Federal district court to compel compliance with the non-

disclosure order. The court has authority to set the terms of a nondisclosure order as appropriate to the circumstances, but must afford substantial weight to the Government's argument in favor of nondisclosure.

Finally, S. 193, as reported, places a sunset on NSL authority. If the sunset were reached under the bill, NSL authority would revert to that statute as of September 10, 2001, prior to enactment of the 2001 USA PATRIOT Act. The sunset was added not as an expression of desire for the authority to expire, but to guarantee that Congress will carefully review how NSLs are issued. An NSL does not need to be presented to a court, a grand jury, or a prosecutor. National Security Letters are typically issued in secret, with recipients silenced under penalty of law. After the standard for issuing an NSL was lowered in 2001, the use of NSLs spiked. Fewer than 10,000 NSLs were issued in 2001, but nearly 50,000 were issued in 2006. Seeing that growth, Congress included Inspector General audits of NSLs in the 2005 USA PATRIOT Act Reauthorization bill. The audits showed vast over-collection of information and abuse of the NSL authority. They also revealed that the FBI used exigent letters over 700 times without proper authorization, and then compounded that misconduct by trying to issue NSLs after the fact to conceal its actions. The bill, therefore, includes the sunset of December 31, 2013, and audits on the use of NSLs.

2. Delayed Notice Search Warrants

a. History of Delayed Notice Search Warrants

Prior to the 2001 USA PATRIOT Act, courts had authorized delayed notice searches in cases where the suspect might flee or destroy evidence. But two leading court decisions required that notice of the search be given within seven days, unless extended by the court. Section 213 of the 2001 USA PATRIOT Act created legislative authorization for delayed notice searches for the first time, but allowed notice to occur within "a reasonable time." During the 2005 USA PATRIOT Act Reauthorization process, Congress imposed the 30-day notice requirement, but still allowed courts to set longer notice periods where justified.

Section 213 of the 2001 USA PATRIOT Act authorized the use of delayed notice, or "sneak and peek," search warrants in criminal cases. These warrants allow law enforcement agents to enter and search an American's home or business, but not notify the owner until weeks or even months later. To obtain such a warrant, the Government must demonstrate to the court that notice would endanger someone's safety, result in flight from prosecution, destruction of evidence, or intimidation of potential witnesses, or otherwise seriously jeopardize an investigation.

Under current law, notice to the owner must be provided within 30 days, or later if the court authorizes it. In addition, the court can extend the time period for additional periods of 90 days, or longer if justified. In addition to the delayed notice search authority in criminal cases, the Government also has the authority under FISA to conduct secret searches of homes and businesses in intelligence investigations without ever providing notice.

Recent reports to Congress from the Administrative Office of the U.S. Courts show that the use of delayed notice search warrants has nearly tripled in the past few years, but that these warrants have been used very rarely in terrorism cases. In fiscal year 2009, Federal prosecutors requested 1,150 delayed notice search warrants and 749 extensions (for a total of 1,899)—up from 419 warrants and 271 extensions (for a total of 690) just two years prior. In addition, only 14 of those 1,899 warrant and extension requests in fiscal year 2009 were made in terrorism cases. In contrast, 1,456 requests were in drug cases.

b. Changes to Delayed Notice Search Warrants Contained in S. 193, as Reported

During the 2009 Senate Judiciary Committee markup of the USA PATRIOT Act Sunset Extension Act, S. 1692, an amendment was offered to require that subjects of delayed notice searches be notified of the search within 7 days, unless a judge grants an extension. It made no other change to the statute other than changing 30 days to 7 days. That amendment is retained as section 11 of S. 193, as reported.

F. RESPONSE TO THE MINORITY VIEWS AND OTHER CLAIMS RAISED DURING COMMITTEE CONSIDERATION OF S. 193

1. Response to Minority Views

There is nothing to support the claim in the Minority Views that the bill somehow creates or rebuilds a "wall" between criminal investigations and intelligence gathering efforts. To the contrary, the bill codifies current practice and makes modest improvements to increase transparency and accountability. None of those improvements impede the operational abilities of law enforcement or the intelligence community to protect against terrorism, or to share information in that effort.

The Minority Views claim that the bill, S. 193, makes "significant changes to existing national security law," which would "increase burdens on investigators" and "result in delays." The Senators who signed the Minority Views claim to "vigorously oppose the changes" contained in the bill and vow to "offer a number of amendments to limit the damage" they assert the bill would cause. These statements are undermined by two objective facts. First, two of the Senators who signed the Minority Views on S. 193, Senators Kyl and Cornyn, voted in favor of reporting a virtually identical bill in the 111th Congress (S. 1962). Second, none of the Senators who signed the Minority Views offered a single amendment during the Committee's consideration of the bill to address any of the provisions of the bill that they now decry as burdensome or otherwise problematic. Rather, they chose to offer amendments that were wholly unrelated to the surveillance issues at the heart of the USA PATRIOT Act. Given the opportunity to strike portions of the bill that they claim to so strenuously oppose, they instead sought to increase penalties for various crimes, create a new death penalty provision for certain crimes, and modify the immigration statute.

The Minority Views also take great pains to suggest that the Department of Justice, FBI, and the intelligence community do not fully support S. 193. References to the personal preference of the

FBI Director and unattributed comments from administration officials do not, however, reflect the collective viewpoint of the administration, including the Department of Justice and the intelligence community. Indeed, at a February 28, 2011, briefing attended by several members of the Committee, including at least three who signed the Minority Views, the Assistant Attorney General for the National Security Division stated that the letters sent by the Attorney General and Director of National Intelligence in 2009 and 2010 expressing the administration's "strong support" for the precursor bill (S. 1692, 111th Congress) remain in force as official statements of administration policy. In the same briefing, the General Counsel to the Director of National Intelligence repeatedly stated that S. 193 is the product of extensive negotiations between the executive branch and Congress and that the bill poses no operational concerns for law enforcement or the intelligence community.

The Minority Views seek to criticize a number of specific provisions of the bill. Responses to these assertions are set forth below.

a. Written Statement of Specific Facts in Support of NSLs: The Minority Views claim that the bill will somehow confuse the FBI by requiring the agency to retain in its files a written statement of specific facts that show reasonable grounds to believe the information sought is relevant to an investigation. The FBI already records a statement of specific facts when it issues an NSL, a practice it adopted to avoid future misuse and abuse of the NSL authority of the type documented by the Inspector General in his March 2007 report on NSLs. See FBI Domestic Investigations and Operations Guide, Section 11.9.3.C.

Taking issue with the word "specific", the Minority Views suggest that this requirement will confuse the FBI and cause operational problems, not unlike the failure of the FBI to obtain a search warrant of Zacharias Moussaoui's computer prior to September 11, 2001. The comparison does not make sense. The FBI failed to obtain a search warrant for Moussaoui's computer because, as Senator Grassley co-wrote in a 2003 Committee report, "key FBI personnel responsible for protecting our country against terrorism did not understand the law." (FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures—An Interim Report by Senators Leahy, Grassley, and Specter, February 2003, at 20, available at http://grassley.senate.gov/releases/2003/p03r02-25c.pdf ("2003 Leahy-Grassley-Specter FISA Report")). The 2003 Leahy-Grassley-Specter FISA Report, which calls throughout for enhanced congressional oversight, attributed this failure to a "fundamental breakdown in training." Id. at 21. The report concluded, "We simply cannot continue to deny or ignore such training flaws only to see them repeated in the future." Id. at 30.

The language in S. 193 regarding retention of a written statement of specific facts directly responds to the failure of the FBI to properly issue NSLs. After the misuse and abuse of NSLs were documented by the Department of Justice Inspector General, the FBI engaged in a process to reform its NSL issuance practice. The bill, S. 193, simply codifies that practice. In short, S. 193 provides assurance that the FBI will follow the law, rather than become confused by it. Finally, it is worth noting that while the Minority Views takes issue with the use of the word "specific", there is ap-

parently no operational or policy concern with requiring the FBI to retain a written statement of facts to support the issuance of NSLs. Again, this is not surprising, given that this is already current FBI practice.

b. Presumption of Relevance in Section 215 Orders: The Minority Views claim that "for reasons that have yet to be fully explained, S. 193 removes the current presumption." The presumption is removed because it was an unnecessary addition to the 2005 USA PATRIOT Act Reauthorization that serves no purpose but to give the Government authority it has not requested be retained. Indeed, David Kris, former Assistant Attorney General for the National Security Division, acknowledged during testimony in September 2009 before this Committee that the relevance standard for obtaining a section 215 order—"with or without the presumption is not a very high standard." It is therefore unsurprising that the minority fails to cite to any facts or sources to support its assertion that the removal of the presumption would somehow lead to delays in drafting applications.

c. Factual Basis for Section 215 Orders and for Pen Registers and Trap and Trace Devices (PR/TT): The Minority Views wrongly claim that a certain phrase added to section 215 orders and PR/TT requirements ("a statement of facts showing reasonable grounds to believe that . . .") will change the standard required to obtain this information by "injecting vague language into a statute depends heavily on its definitions." In fact identical language is used in Title I and Title III of FISA. To ensure that the new language is not interpreted to raise the standard, the sectional analysis in this Committee Report states the clear intent to neither affect nor restrict any activities approved by the FISA Court. This same report language was included in the Committee Report for S. 1692 from the 111th Congress. The Department of Justice, FBI, and Director of National Intelligence have all endorsed this language.

d. Library and Bookseller Records: The Minority Views assert that the standard for obtaining library and bookseller records under the reported version of S. 193 will create an "open invitation to terrorists to use unsuspecting third parties to communicate with associates." Yet this requirement, which was supported by the Chairman of the Intelligence Committee, Senator Feinstein, is already being implemented by the Attorney General as indicated in his December 9, 2010 letter to Chairman Leahy. Although the Minority Views suggest that the section 215 standard for library and bookseller records under S. 193 could have impeded the FBI investigation of Khalid Aldawsari, the individual arrested on terrorism-related charges in Texas on February 23, 2011, the Attorney General noted in his December 2010 letter to Chairman Leahy that it is already current FBI practice to provide the FISA Court with a complete statement of facts to support issuance of a section 215 order.

e. FISA Court Review of Section 215 Minimization: The Minority Views complain that FISA Court review of minimization might lead to differing minimization requirements being applied to different cases. This claim ignores the practice of the FISA Court, which has already approved minimization standards for section 215 orders. The language in S. 193 simply codifies current practice, required by statute under 50 U.S.C. § 1861(b)(2)(B), a fact confirmed in the

December 9, 2010 letter from the Attorney General to Chairman Leahy.

f. Delayed Notice Warrants: The Minority Views claim that S. 193 will hamper law enforcement by changing the period of time after which the Government must inform the target of a delayed notice search warrant from 30 days to 7 days. The Government can, and often does seek extensions of these orders. The administration endorsed this provision, noting that as long as extensions may be sought from a court, it does not oppose modifying the number of days prior to notification.

2. Response to other claims raised during committee consideration of S. 193

During Committee consideration of S. 193, opponents of the bill suggested that no evidence has been provided to the Committee to justify changes to current law. In fact, several modifications to current law contained in the bill are the result of problems discovered by the Department of Justice Inspector General in reports and audits. As noted above, the Department of Justice Inspector General found extensive evidence of misuse of National Security Letters. A March 2007 report "concluded that the FBI engaged in serious misuse of NSL authority," including improper authorization of NSLs, improper requests under the pertinent national security letter statutes, and unauthorized collections. The report also identified more than 700 instances in which the FBI improperly obtained telephone records by issuing "exigent letters." The Department of Justice Inspector General also found a small number of instances in which improper use of section 215 orders by the FBI resulted in over-collection of information. The bill codifies the changes in practice by the FBI that will prevent such misuse from occurring in the future, and builds in an audit trail so that both the FBI and the Department of Justice Inspector General can monitor future compliance.

Another assertion raised in the markup is that there has been no situation in which prosecutors overstepped their authority and were overruled by a court. The United States Court of Appeals for the Second Circuit found constitutional defects in current law restricting the ability of a recipient of a nondisclosure order on an NSL to challenge that nondisclosure order. See *Doe* v. *Mukasey*, 549 F.3d 861 (2d Cir. 2008). To correct the constitutional infirmity, the bill adopts the concepts suggested by that court for a constitutionally sound process. This provision of the bill should be uncontroversial. Similar language was introduced as part of a bill sponsored by Senators Sessions, Bond (R–MO), and Lieberman (ID–CT) in the 111th Congress. (See section 4 of S. 2336, 111th Cong.)

The majority of legal review of surveillance authorities takes place before the FISA Court, away from public scrutiny. Yet in April 2009, the Department of Justice confirmed to the press that "there had been problems with the NSA surveillance operation." The Department of Justice also confirmed that Attorney General Holder went to the FISA Court to seek a renewal of the surveillance program only after new safeguards were put in place. Several intelligence officials told the press that "the N.S.A. had been engaged in 'overcollection' of domestic communications of Americans."

(New York Times, "Officials Say U.S. Wiretaps Exceeded Law," April 16, 2009.)

Additional reforms and improvements to the USA PATRIOT Act are necessary. To say otherwise is to ignore the facts. The FBI has made progress in addressing the problems documented by the Department of Justice Inspector General, but the positive steps it has taken should be codified in statute to ensure that mistakes are not made in the future. By the same token, a lack of evidence of abuse does not suggest that surveillance provisions should be made permanent, particularly when one of those provisions—the "lone wolf" provision—has never even been used, and therefore is not susceptible to review. The purpose of the sunsets in the bill is to guarantee that Congress will carefully review the use and effect of laws that authorize surveillance of Americans. The version of the USA PATRIOT Act Sunset Extension Act that the Committee reported in 2009 was virtually identical to the 2011 version and received bipartisan support, with Senators Kyl and Cornyn voting in favor of reporting the bill to the full Senate. The 2011 version of the bill, S. 193, also received a bipartisan vote, with Senator Lee voting in favor of the bill.

II. HISTORY OF THE BILL AND COMMITTEE CONSIDERATION

A. INTRODUCTION OF THE BILL

The USA PATRIOT Act Sunset Extension Act of 2011 was introduced as S. 193 on January 26, 2011 by Senator Leahy.

B. COMMITTEE CONSIDERATION

Executive Business Meetings

The bill was placed on the Committee's agenda for consideration on February 3, 2011. It was held over on that date.

On February 17, 2011, the Committee on the Judiciary considered S. 193 during an executive business meeting. Chairman Leahy offered an amendment to modify the due dates of the audits contained in section 10 of S. 193. The amendment was accepted by consent.

Senator Feinstein offered an amendment to extend the sunsets in the FISA Amendments Act of 2008 (Pub. L. No. 110–261), from December 31, 2012, to December 31, 2013. Therefore, if S. 193, as amended is enacted, the sunsets in the USA PATRIOT Act and the sunsets in the FISA Amendments Act of 2008 will be aligned to expire on the same date. The amendment was accepted by consent.

Senator Leahy offered an amendment regarding the standard for obtaining bookseller records under section 215 of the USA PATRIOT Act to the bill, to match the requirement already contained in the bill for library records. The Committee adjourned prior to disposing of the amendment. Senator Grassley objected to completing consideration of the amendment and requested that the Chairman arrange a classified briefing with officials from the Department of Justice and the intelligence community. A classified briefing for members of the Committee was provided on February 28, 2011, by officials from the Department of Justice, the Office of the Director of National Intelligence, and the National Security Agency.

On March 10, 2011, the Committee on the Judiciary resumed consideration of S. 193.

Senator Leahy offered a technical amendment to modify S. 193 to reflect the fact that Congress enacted a short term extension of the expiring provisions from February 28, 2011, to May 27, 2011. The amendment was accepted by consent.

Senator Leahy then offered a modified version of the bookseller amendment he previously offered on February 17, 2011. The new version was virtually identical to the earlier bookseller amendment, but struck the phrase "and articulable" from the phrase "specific and articulable facts" to conform the amendment to the language in the underlying bill relating to section 215 orders. The amendment was accepted by a roll call vote.

The vote record is as follows:

Tally: 11 Yeas, 7 Nays

Yeas (11): Kohl (D–WI), Feinstein (D–CA), Schumer (D–NY), Durbin (D–IL), Whitehouse (D–RI), Klobuchar (D–MN), Franken (D–MN), Coons (D–DE), Blumenthal (D–CT), Lee (R–UT), Leahy (D–VT).

Nays (7): Grassley (R–IA), Hatch (R–UT), Kyl (R–AZ), Sessions (R–AL), Graham (R–SC), Cornyn (R–TX), Coburn (R–OK).

Senator Grassley offered an amendment to add the death penalty as a punishment to certain crimes involving weapons of mass destruction. Senator Leahy offered a motion to table the amendment. The motion to table was rejected by a roll call vote.

The vote record is as follows:

Tally: 7 Yeas, 10 Nays, 1 Pass

Yeas (7): Durbin (D–IL), Whitehouse (D–RI), Klobuchar (D–MN), Franken (D–MN), Coons (D–DE), Blumenthal (D–CT), Leahy (D–-VT).

Nays (10): Feinstein (D–CA), Schumer (D–NY), Grassley (R–IA), Hatch (R–UT), Kyl (R–AZ), Sessions (R–AL), Graham (R–SC), Cornyn (R–TX), Lee (R–UT), Coburn (R–OK).

Pass (1): Kohl (D–WI).

The Grassley amendment was then accepted by voice vote.

Senator Durbin offered an amendment cosponsored by Senator Lee to modify the "roving" wiretap statute to require that the Government describe the target of FISA surveillance with particularity. The amendment was accepted by roll call vote.

The vote record is as follows:

Tally: 11 Yeas, 7 Nays

Yeas (11): Kohl (D–WI), Feinstein (D–CA), Schumer (D–NY), Durbin (D–IL), Whitehouse (D–RI), Klobuchar (D–MN), Franken (D–MN), Coons (D–DE), Blumenthal (D–CT), Lee (R–UT), Leahy (D–VT).

Nays (7): Grassley (R–IA), Hatch (R–UT), Kyl (R–AZ), Sessions (R–AL), Graham (R–SC), Cornyn (R–TX), Coburn (R–OK).

Senator Cornyn offered an amendment to modify the immigration statute to add terrorism to the list of characteristics that bar an alien from applying to naturalize or seek other immigration benefits because of a lack of good moral character. Senator Leahy offered a motion to table the amendment. The motion to table was accepted by a roll call vote.

The vote record is as follows:

Tally: 10 Yeas, 8 Nays

Yeas (10): Kohl (D–WI), Feinstein (D–CA), Schumer (D–NY), Durbin (D–IL), Whitehouse (D–RI), Klobuchar (D–MN), Franken (D–MN), Coons (D–DE), Blumenthal (D–CT), Leahy (D–VT).

Nays (8): Grassley (R–IA), Hatch (R–UT), Kyl (R–AZ), Sessions (R–AL), Graham (R–SC), Cornyn (R–TX), Lee (R–UT), Coburn (R–OK).

Senator Whitehouse offered a conforming amendment to strike the words "and articulable" from the section of S. 193 regarding judicial review of NSLs. Under the revised language, the bill would require the applicant for a nondisclosure order accompanying an NSL to include a statement of specific facts indicating that nondisclosure is necessary to prevent a danger to national security or other enumerated harms. The amendment was accepted by voice vote.

Senator Kyl offered three amendments that would have increased penalties and added mandatory minimum sentences for crimes involving terrorism hoaxes, sexual assault, kidnapping, and suicide bombing, among others. Senator Kyl withdrew the amendments.

The Committee then voted to report the USA PATRIOT Act Sunset Extension Act, as amended, favorably to the Senate. The Committee proceeded by roll call vote as follows:

Tally: 11 Yeas, 7 Nays

Yeas (10): Kohl (D–WI), Feinstein (D–CA), Schumer (D–NY), Durbin (D–IL), Whitehouse (D–RI), Klobuchar (D–MI), Franken (D–MI), Coons (D–DE), Blumenthal (D–CT), Lee (R–UT), Leahy (D–VT).

Nays (7): Grassley (R–IA), Hatch (R–UT), Kyl (R–AZ), Sessions (R–AL), Graham (R–SC), Cornyn (R–TX), Coburn (R–OK).

III. SECTION-BY-SECTION SUMMARY OF THE BILL

Section 1. Short title

This section provides that the legislation may be cited as the "USA PATRIOT Act Sunset Extension Act of 2011."

Section 2. Sunsets

This section extends the sunsets on the provisions for "lone wolf," roving wiretaps and orders for tangible things from May 27, 2011 to December 31, 2013. This section establishes a sunset of December 31, 2013, on the use of NSLs. This section also changes the sunset dates for provisions under the FISA Amendments Act of 2008 (Pub. L. No. 110–261) from December 31, 2012 to December 31, 2013. This section also makes conforming amendments to FISA and other applicable laws consistent with the sunsets.

Section 3. Factual basis for and issuance of orders for access to tangible things

This section modifies the standard for obtaining a court order for tangible things under FISA. Current law requires the Government to submit a statement of facts showing reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation. However, current law states that the tangible things sought are presumptively relevant if the Government shows that they pertain to (a) a foreign power or an agent of a foreign power,

(b) the activities of a suspected agent of a foreign power who is the subject of such an authorized investigation, or (c) an individual in contact with, or known to, an agent of a foreign power who is the subject of such authorized investigation. This section removes the presumption of relevance described above. It requires the Government to provide a statement of the facts and circumstances relied upon by the applicant to justify the applicant's belief that the tangible things sought are relevant. This ensures that the Government is presenting a thorough statement of facts to the court and strengthens judicial oversight. The Department of Justice has indicated that it does not rely on this presumption, and that its current practice is to provide the Foreign Intelligence Surveillance Court with a complete statement of facts to support issuance of an order.

Section 3(a)(2)(A) alters certain requirements with respect to applications made pursuant to 50 U.S.C. § 1861. These changes are not intended to affect or restrict any activities approved by the FISA Court under existing statutory authorities. Rather, this provision is intended to ensure that in applications made pursuant to 50 U.S.C. § 1861, the Government must submit a statement of the facts it relies on to support its belief that the items or information sought are relevant to an authorized investigation and that such relevance is not to be presumed based on the presence of certain factors.

To obtain library records that contain personally identifiable information about a patron, or bookseller records, the Government must provide a statement of facts showing reasonable grounds to believe the tangible things are relevant to an authorized investigation and pertain to (a) an agent of a foreign power, (b) the activities of a suspected agent, or (c) an individual in contact with or known to a suspected agent of foreign power subject to the investigation. "Bookseller records" are defined as meaning any transactional records reflecting the purchase or rental of books, journals, or magazines, whether in digital or print form. The Department of Justice has already agreed to implement this requirement administratively.

This section also requires court review of minimization procedures. Finally, this section includes transition procedures to ensure that any order in effect at the time of enactment remains in effect until the expiration of the order.

Section 4. Factual basis for and issuance of orders for pen registers and trap and trace devices for foreign intelligence purposes

Under current law, in order to obtain a FISA pen/trap, the Government must certify that the information sought is merely foreign intelligence information or is relevant to an investigation to protect against terrorism. The bill modifies the standard for obtaining a pen/trap to require the Government to provide a statement of the facts and circumstances relied upon by the applicant to justify the applicant's belief that the information likely to be obtained is relevant. This ensures that the Government is presenting a thorough statement of facts to the court and strengthens judicial oversight.

Section 4(a)(2)(A) alters certain requirements with respect to applications made pursuant to 50 U.S.C. § 1842. These changes are not intended to affect or restrict any activities approved by the FISA Court under existing statutory authorities. Rather, this provi-

sion is intended to ensure that in applications made pursuant to 50 U.S.C. § 1842, the Government must submit a statement of the facts it relies on to support its belief that the items or information sought are relevant to an authorized investigation.

This section also requires minimization procedures, which are not required under current law, and makes those procedures subject to court review. Section 4(b) governs procedures for minimization of the retention and dissemination of information obtained pursuant to 50 U.S.C. § 1842 where appropriate in exceptional circumstances. This provision is intended to provide a statutory footing for the existing practice whereby specialized minimization procedures are implemented in certain limited circumstances under FISA Court authorization and oversight.

Finally, this section includes transition procedures to ensure that any order in effect at the time of enactment remains in effect until the expiration of the order.

Section 5. Limitations on disclosure of national security letters

This section authorizes the Government to prohibit disclosure of the receipt of an NSL (there are four different statutes that authorize NSLs) where a high level official certifies that disclosure may result in danger to the national security, interference with an investigation, or danger to the life or safety of a person. The FBI has stated that its current practice is to require such a certification to include an appropriately thorough statement of facts setting forth the need for nondisclosure.

The recipient of an NSL nondisclosure order may challenge the nondisclosure at any time by notifying the Government of a desire to not comply. Section 6 (below) details the process for doing so.

Section 6. Judicial review of FISA orders and NSL nondisclosure orders

This section allows the recipient of a section 215 order for tangible things to challenge the order itself and any nondisclosure order associated with it. Current law requires a recipient to wait a year before challenging a nondisclosure order. This section repeals that one-year mandated delay before a recipient of an order for tangible things can challenge such a nondisclosure order in court. It also repeals a provision added to the law in 2006 stating that a conclusive presumption in favor of the Government shall apply where a high level official certifies that disclosure of the order for tangible things would endanger national security or interfere with diplomatic relations.

This section also corrects the constitutional defects in the issuance of nondisclosure orders on NSLs as found by the Second Circuit Court of Appeals in *Doe* v. *Mukasey*, 549 F.3d 861 (2d Cir. 2008), and adopts the concepts suggested by that court for a constitutionally sound process. Id. at 883–84. The bill allows the recipient of an NSL with a nondisclosure order to notify the Government at any time that it wishes to challenge the nondisclosure order. The Government then has 30 days to seek a court order in Federal district court to compel compliance with the nondisclosure order. The court has authority to set the terms of a nondisclosure order as appropriate to the circumstances, but must afford substantial weight to the Government's argument in favor of nondisclosure.

According to current Department of Justice policy, all NSLs must include a notice that informs recipients of the opportunity to contest the nondisclosure requirement through the Government-initiated judicial review. This section states that the government's application for an NSL nondisclosure order may be filed either in the district within which the authorized investigation is conducted or in the jurisdiction where the recipient's business is located. This option will ease the burden on the recipient in challenging the nondisclosure order.

This section requires the Government to notify any entity that challenges a nondisclosure order when the need for nondisclosure is terminated. The Department of Justice agreed to implement this measure administratively in December 2010; therefore, this section will codify current practice.

The bill also requires FISA Court approval of minimization procedures in relation to the issuance of a section 215 order for production of tangible things, similar to the court approval required for other FISA authorities such as wiretaps, physical searches, and pen register and trap and trace devices.

Section 7. Certification for access to telephone toll and transactional records

This section codifies current FBI practice in issuing an NSL, and augments oversight and transparency. Current law requires only that an official certify that the information requested in the NSL is relevant to, or sought for, an authorized investigation to protect against international terrorism or clandestine intelligence activities, or for a law enforcement investigation, counterintelligence inquiry, or security determination. This section adds a requirement that the FBI retain a written statement of specific facts showing that there are reasonable grounds to believe that the information sought is relevant to such an authorized investigation. This statement of specific facts will not be included in the NSL itself, but will be available for internal review and Office of Inspector General audits. The Department of Justice has stated that it is current policy for the FBI to retain a statement of specific facts showing the information sought through NSLs is relevant to an authorized investigation.

Section 8. Public reporting on national security letters

This section requires reporting of aggregate numbers based upon the total number of all NSLs issued each year, as opposed to by individual NSL. This section ensures that the FBI can keep an accurate record of the information it must disclose by allowing it to report both on persons who are the subject of an authorized national security investigation, and on individuals who have been in contact with or otherwise directly linked to the subject of an authorized national security investigation.

Section 9. Public reporting on the Foreign Intelligence Surveillance Act

This section requires that the Government produce an annual unclassified report on how the authorities under FISA are used, including their impact on the privacy of United States persons. This report shall be easily accessible on the Internet.

Section 10. Audits

This section requires the DOJ Office of Inspector General to conduct audits of the use of three surveillance tools: (1) orders for tangible things under section 215 of the 2001 Patriot Act, or section 501 of FISA; (2) pen registers and trap and trace devices under section 402 of FISA; and (3) the use of NSLs. The audits will cover the years 2007 through 2011. The scope of such audits includes a comprehensive analysis of the effectiveness and use of the investigative authorities provided to the Government, including any improper or illegal use of such authorities. This section also requires the Inspectors General of the Intelligence Community to submit separate reports that also review these three provisions. The audits covering the years 2007–2009 must be completed by March 31, 2012. The audits for the years 2010–2011 must be completed by March, 31, 2013. These due dates ensure that Congress will have time to fully consider the findings of the audits prior to the December 31, 2013 sunsets in the bill.

Section 11. Delayed notice search warrants

Current law requires notification of a delayed notice search warrant within 30 days. This section requires notification of a delayed notice search warrant within seven days, or a longer period if justified.

Section 12. NSL procedures

Current law does not require minimization procedures be established, but on October 1, 2010, the Attorney General adopted procedures concerning the collection, use, and storage of information obtained in response to NSLs. This section requires that the Attorney General periodically review, and revise as necessary, those procedures, and to give due consideration to the privacy interests of individuals and the need to protect national security. If the Attorney General makes any significant changes to these NSL procedures, the Attorney General is required under this section to notify Congress, and to submit a copy of the changes.

Section 13. Severability

This section includes a severability clause that will ensure that in the event any part of the bill or any amendment to the bill is found to be unconstitutional the remainder of the bill will not be affected.

Section 14. Offset

This section includes a $5,000,000 offset from the Department of Justice Assets Forfeiture Fund for any direct spending that could be incurred by the provisions of the bill.

Section 15. Electronic surveillance

This section is intended to amend the FISA wiretap statute (50 U.S.C. § 1805(c)(1)(A)) so as to require law enforcement to identify "with particularity" the target of a wiretap request under FISA. The Department of Justice has testified that, in applications to the FISA Court for "roving" wiretaps, it must provide the court sufficient detail to identify the target with particularity.

Section 16. Death penalty for certain terror related crimes

This section provides for the possibility of the death penalty as punishment for certain crimes involving the use of weapons of mass destruction, including nuclear weapons, missile systems, radiological devices, and the variola virus.

Section 16. Effective date

This section includes an effective date of 120 days from the date of enactment for the statutory revisions made by this legislation to take effect. This period of time will provide the Government an appropriate amount of time to implement the new procedures required by the legislation.

IV. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

The Committee sets forth, with respect to the bill, S. 193, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

MARCH 31, 2011.

Hon. PATRICK J. LEAHY,
Chairman, Committee on the Judiciary,
U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 193, the USA PATRIOT Act Sunset Extension Act of 2011.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Grabowicz.

Sincerely,

DOUGLAS W. ELMENDORF.

Enclosure.

S. 193—USA PATRIOT Act Sunset Extension Act of 2011

Summary: The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (Public Law 107–56), the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108–458), and the USA PATRIOT Improvement and Reauthorization Act of 2005 (Public Law 109–177) expanded the powers of federal law enforcement and intelligence agencies to investigate and prosecute terrorist acts. S. 193 would extend, until December 31, 2013, certain provisions of those acts that will otherwise expire in 2011. In addition, the bill would require the Department of Justice (DOJ) and certain offices within the intelligence community to prepare additional reports and audits relating to those investigations. Finally, S. 193 would permanently rescind $5 million from the unobligated balances of DOJ's Assets Forfeiture Fund.

Assuming appropriation of the necessary amounts, CBO estimates that implementing S. 193 would have discretionary costs of $9 million over the 2011–2016 period. We also estimate that enacting the legislation would decrease direct spending by $5 million over the 2011–2013 period (with no impact after 2013). In addition, we estimate that enacting the bill would affect revenues, but such effects would not be significant. Pay-as-you-go procedures apply be-

cause enacting the legislation would affect direct spending and revenues.

CBO has determined that the provisions of S. 193 are either excluded from review for mandates under the Unfunded Mandates Reform Act (UMRA) because they are necessary for national security or they contain no intergovernmental or private-sector mandates.

Estimated cost to the Federal Government: The estimated budgetary impact of S. 193 is shown in the following table. The costs of this legislation fall within budget functions 050 (national defense) and 750 (administration of justice).

	By fiscal year, in millions of dollars—						
	2011	2012	2013	2014	2015	2016	2011–2016
CHANGES IN DIRECT SPENDING							
Budget Authority	-5	0	0	0	0	0	-5
Estimated Outlays	-1	-2	-2	0	0	0	-5
CHANGES IN SPENDING SUBJECT TO APPROPRIATION							
Estimated Authorization Level	1	4	3	*	*	*	9
Estimated Outlays	1	4	3	*	*	*	9

Note: * = less than $500,000.

Basis of estimate: For this estimate, CBO assumes that the bill will be enacted by July 1, 2011, and that the amounts necessary to implement the bill will be appropriated for each year.

Direct spending and revenues

S. 193 would permanently rescind $5 million from the unobligated balances of the DOJ Assets Forfeiture Fund. CBO estimates that this rescission would reduce direct spending by $1 million in 2011 and by $2 million in each of fiscal years 2012 and 2013.

Because those prosecuted and convicted under S. 193 could be subject to civil and criminal fines, the federal government might collect additional fines if the legislation is enacted. Collections of civil fines are recorded in the budget as revenues. Criminal fines are recorded as revenues, deposited in the Crime Victims Fund, and later spent. CBO expects that any additional revenues and direct spending would not be significant because of the small number of cases likely to be affected.

Spending subject to appropriation

We estimate that implementing the bill would cost about $9 million over the 2011–2016 period, assuming appropriation of the necessary amounts. S. 193 would require the inspectors general of DOJ and certain offices within the intelligence community, by March 31, 2013, to conduct audits of their agencies' use of selected investigative powers during the 2007–2011 period. The bill also would require DOJ to prepare new reports each year, in both classified and unclassified form, on its use of certain investigative powers.

Based on information from DOJ and the intelligence community, we expect that about two dozen people would be hired to carry out the audits and prepare the reports. CBO estimates that it would cost about $1 million in fiscal year 2011, $4 million in 2012, $3 mil-

lion in 2013, and less than $500,000 annually thereafter to complete the audits and reports required by the bill.

Pay-As-You-Go considerations: The Statutory Pay-As-You-Go Act of 2010 establishes budget-reporting and enforcement procedures for legislation affecting direct spending or revenues. By rescinding $5 million from the unobligated balances of the Assets Forfeiture Fund, S. 193 would reduce direct spending. The bill also could affect direct spending and revenues through the collection and spending of civil and criminal fines. The net changes in outlays and revenues that are subject to those pay-as-you-go procedures are shown in the following table.

CBO ESTIMATE OF PAY-AS-YOU-GO EFFECTS FOR S. 193 AS REPORTED BY THE SENATE COMMITTEE ON THE JUDICIARY ON MARCH 17, 2011

	By fiscal year, in millions of dollars—												
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2011–2016	2011–2021
NET INCREASE OR DECREASE (·) IN THE DEFICIT													
Statutory Pay-As-You-Go Impact	·1	·2	·2	0	0	0	0	0	0	0	0	·5	·5
Memorandum:													
Changes in Outlays	·1	·2	·2	0	0	0	0	0	0	0	0	·5	·5
Changes in Revenues	0	0	0	0	0	0	0	0	0	0	0	0	0

Intergovernmental and private-sector impact: CBO has determined that the provisions of S. 193 are either excluded from review for mandates under UMRA because they are necessary for national security or they contain no intergovernmental or private-sector mandates.

Estimate prepared by: Federal Costs: Mark Grabowicz (DOJ) and Jason Wheelock (Intelligence Community); Impact on State, Local, and Tribal Governments: Melissa Merrell; Impact on the Private Sector: Paige Piper/Bach.

Estimate approved by: Theresa Gullo, Deputy Assistant Director for Budget Analysis.

V. REGULATORY IMPACT EVALUATION

In compliance with rule XXVI of the Standing Rules of the Senate, the Committee finds that under S. 193, as reported, the Department of Justice would be required to issue minimization procedures on section 215 orders, and pen register and trap and trace devices.

VI. CONCLUSION

The USA PATRIOT Act Sunset Extension Act of 2011, S. 193, was reported favorably to the Senate with a bipartisan vote from the Committee on the Judiciary. The bill provides the Government with important tools to prevent terrorist attacks, while increasing protections of civil liberties, and affording greater respect for constitutional rights than under current law. The bill contains vigorous oversight and public reporting requirements, new Inspector General audits, and sunsets on four controversial provisions. Because three provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 are due to expire on May 27, 2011, the Committee recommends swift action on S. 193 as reported.

VII. MINORITY VIEWS

MINORITY VIEWS FROM SENATORS GRASSLEY, HATCH, KYL, SESSIONS, GRAHAM, CORNYN, AND COBURN

Prior to September 11, 2001, government surveillance authorities fell, broadly, into two categories: ordinary domestic crime and foreign intelligence information collection. A rigid divide between the two undermined the government's ability to "connect the dots" in terrorism investigations because it prevented domestic law enforcement officers from collaborating with national security personnel. To protect against future threats to our security, government investigators needed more appropriate counterterrorism and foreign intelligence tools. As a result, Congress enacted the USA PATRIOT Act[4] among other legislative responses.

If Congress does not act in the coming weeks, three vital national security tools to fight terrorism and prevent attacks will expire.[5] These provisions, section 206 of the USA PATRIOT Act authorizing roving wiretaps, section 215 of the USA PATRIOT Act regarding access to tangible things such as business records, and section 6001 of the Intelligence Reform and Terrorism Prevention Act, otherwise known as the "lone wolf" provision, have previously been reauthorized and there have been no reported abuses of these authorities.[6] These tools, established in the wake of the September 11th attacks, have helped federal law enforcement and intelligence agencies stay ahead of terrorists to prevent or thwart planned attacks.

A key theme of these post-9/11 provisions was the purposeful dismantling of the distinctions between criminal and national security investigative tools. Congress believed then, as we believe now, that an FBI agent investigating a potential act of terrorism should have the same tools and authorities available to an FBI agent investigating a drug offense. While there are some distinctions that remain in place between criminal and national security tools, the effort to have greater parity among them has been largely successful. For example, section 206 of the PATRIOT Act gives intelligence agencies a capability that has been available to law enforcement for decades. Unfortunately, S. 193 puts us back on a path to a pre-9/11 mindset, in which arbitrary distinctions between criminal and

[4] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107–56, 115 Stat. 272 (Oct. 26, 2001).

[5] These provisions were set to expire at the February 28, 2011, but Congress passed Pub. L. No. 112–3, 125 Stat. 5 (Feb. 25, 2011), a short term extension which extends the provisions until May 27, 2011.

[6] U.S. Dep't of Justice, Office of the Inspector Gen., A Review of the FBI's Use of Section 215 Orders for Business Records in 2006, at 5 March 2008 noting, "We did not identify any illegal use of Section 215 authority."

national security techniques were the norm. This we cannot sanction.

On January 26, 2011, Senator Leahy introduced S. 193, the USA PATRIOT Act Sunset Extension Act of 2011. This legislation is similar to previous legislation he introduced that was reported out of the Judiciary Committee (Committee) in the 111th Congress,[7] but not considered on the Senate floor. S. 193 reauthorizes expiring provisions of the PATRIOT Act, but with significant changes to existing national security law. These changes would increase burdens on investigators, result in delays—seldom experienced in domestic criminal matters—in obtaining critical national security authorities, and drain federal resources that should be focused on keeping the nation safe. If S. 193 becomes law, national security investigators will face greater procedural hurdles to using critical surveillance tools—many of which have long been readily available to law enforcement in run-of-the-mill criminal cases.

S. 193 makes significant changes to the three expiring provisions and other critical national security tools, despite the fact that we currently face an ongoing and evolving terrorist threat. For example, the General Counsel for the Office of the Director of National Intelligence recently testified before the House Judiciary Committee: "The threat to the Homeland from violent extremists is growing . . . the nature of the terrorism threat that we face is evolving. Our adversaries are constantly adapting their strategies and communication techniques."[8] The Attorney General also recently stated, "The threat has changed from simply worrying about foreigners coming here, to worrying about people in the United States, American citizens—raised here, born here, and who for whatever reason, have decided that they are going to become radicalized and take up arms against the nation in which they were born."[9] Federal Bureau of Investigation (FBI) Director Mueller stated, "Threats from homegrown terrorists are also of great concern. These individuals are harder to detect, easily able to connect with other extremists on the Internet, and—in some instances—highly capable operationally."[10]

We raise our concerns with S. 193 against this backdrop of evolving terrorist threats, including the deadly shooting at Fort Hood by Major Nidal Hassan, and recent attempted terrorist attacks that fortunately were thwarted before any lives were lost. Among the thwarted attacks: the February 2011 plot by Khalid Ali-M Aldawsari in Lubbock, Texas, to utilize weapons of mass destruction; the 2009 plot by Najibullah Zazi to bomb the New York City subway; the failed bombing in Times Square by Faisal Shahzad; the planned bombing of the Washington D.C. Metro system by Farooque Ahmed; and the failed bombing of Northwest Airlines Flight 253 on Christmas Day 2009 by Umar Farouk Abdulmutallab. These thwarted attacks make clear that our en-

---

[7] The USA PATRIOT Act Sunset Extension Act of 2009, S. 1692, 111th Cong. (2009).

[8] USA PATRIOT Act Reauthorization: Hearing Before the Subcomm. On Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong. (March 9, 2011) (statement of Robert S. Litt, General Counsel, Office of the Dir. Of Nat'l Intelligence).

[9] Good Morning America, Interview of Attorney General Eric H. Holder, Jr. (ABC television broadcast Dec. 21, 2010).

[10] Federal Bureau of Investigation Director Robert S. Mueller, III, Address at the 10th Annual Int'l Ass'n of Chiefs of Police Conference Orlando, FL (Oct. 25, 2010).

emies have not rested since 9/11, but remain intent upon causing us harm—including here at home. Because now is not the time to be dialing back or raising the bar on any of our national security tools, we agree with FBI Director Robert Mueller's statement to the House Judiciary Committee on March 16, 2011 that we favor reauthorization of the three expiring provisions as is.

The Three Expiring Provisions

The PATRIOT Act has provided our national security investigators and analysts with critical legal authorities they need to protect the nation against terrorist threats. These legal tools were authorized in 2001, then renewed as part of the PATRIOT Act reauthorization in 2005 and 2006, and then again in December 2009. Three provisions are currently set to expire on May 28, 2011. These three provisions are:

- The "roving wiretap" provision, Section 206 of the USA PATRIOT Act. This tool allows investigators to collect evidence against terrorists in the same way that evidence is collected against drug dealers in the criminal context, and requires an initial finding of probable cause by the court. Retaining the ability to maintain surveillance on terrorists who are trained to evade detection is crucial, particularly in the age of disposable cell phones, which terrorists are known to use and frequently replace. The current authority already sets forth a process for notification to the court when a terrorist is tracked using roving authority. This process enables agents to continue their investigation, without having to file repetitious court applications every time a terrorist changes phones. Like regular wiretaps, roving wiretaps have been routinely used in domestic law enforcement for decades.
- The "business records" authority, Section 215 of the USA PATRIOT Act. This authority allows officials to *ask a court for an order* to obtain tangible things, including business records, in national security terrorism cases. Examining business records often provides key information that assists investigators in solving a wide range of crimes. In criminal matters, similar records may be obtained using a grand jury subpoena, without any need for court approval.
- The "lone wolf" authority, Section 6001 of the Intelligence Reform and Terrorism Prevention Act. This authority allows intelligence investigations of terrorists who cannot initially be connected to a foreign power or terrorist organization. Before 2004, national security officials had to show a court that a target was an agent of a foreign power, or acting on behalf of a foreign power, in order to get permission to monitor him. This was a problem in the case of Zacharias Moussaoui (the so-called "20th hijacker" in the 9/11 attacks), when agents did not get a search warrant for his computer because they believed that they could not show that he was an agent of a foreign power.

All three of these authorities were previously reauthorized by 89 Senators—including President Obama and Vice President Biden when they were senators in 2006. Despite the fact that these provisions have not been abused, S. 193 would continue to include sunsets on these authorities and would make a host of changes to

other counter-terrorism and counter-intelligence authorities that increase the burdens associated with utilizing them.

S. 193 Unduly Expands Burdens on Expiring Provisions

Chief among our concerns are the increased requirements that S. 193 would place on existing surveillance authorities. The Foreign Intelligence Surveillance Act (FISA) is a precisely worded statute where certain words have longstanding and carefully crafted definitions that impact how those in the intelligence community do their jobs. Adding words or phrases to portions of FISA that are undefined or vague can have serious and unintended consequences on those operating in the field. Further, the FISA court already has the authority to require additional documentation or data to support orders in specific cases sought by the intelligence community. Changing the statutory requirements, regardless of whether the Court is already exercising its discretion by requiring such information, will certainly impact how the Department of Justice prepares applications before they are submitted to the court.

Generally stated, we have serious concerns with how S. 193 would increase the burdens on law enforcement and intelligence community personnel and create new divisions between criminal and intelligence authorities—potentially rebuilding the "wall" between criminal and intelligence collection. We are concerned that additional requirements will inherently slow down the process for obtaining critical intelligence in early stages of counter-intelligence and counter-terrorism investigations. We offer the following details to support our concerns.

1. Increases the Burden to Obtain Business Records from Third Parties

Section 215 of the PATRIOT Act concerns the government's ability to obtain business records from third parties, such as banking information and car rental agreements. Under Supreme Court precedent, business records, such as banking deposit slips or car rental records are not subject to Fourth Amendment protections because the customer has no reasonable expectation of privacy in documents that are in the possession of third parties.[11] Because obtaining such records is not a search under the Fourth Amendment, prosecutors in standard criminal investigations can seek these types of records through the use of a simple grand jury subpoena.

Under current law, however, investigators pursuing terrorists and spies face the additional burden of seeking court permission to obtain similar records. Other distinctions also exist. A 215 order cannot be based solely on First Amendment protected activities.[12] Further, only three specified, high-ranking federal officials have the authority to request these orders in certain sensitive areas—such as library records.[13] Thus, under current law, this section puts greater burdens on law enforcement in terrorism cases than otherwise apply to standard criminal law enforcement.

Despite the already more difficult process in the terrorism context, S. 193 further increases the elements of proof needed to ob-

[11] *U.S.* v. *Miller*, 425 U.S. 435 (1976).
[12] *See* 50 U.S.C. § 1861(a)(2)(B) (2006).
[13] 50 U.S.C. § 1861(a)(3) (2006).

tain business records under Section 215. Current law requires the government to submit a statement of facts showing reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation.[14] Current law also states that tangible things sought are presumptively relevant if the government shows they pertain to (a) a foreign power or agent of a foreign power, (b) the activities of a suspected agent of a foreign power who is the subject of such an authorized investigation, or (c) an individual in contact with, or known to, an agent of a foreign power who is the subject of such authorized investigation.[15] For reasons that have yet to be fully explained, S. 193 removes the current presumption of relevance.

The presumption of relevance was included in Section 215 originally in order to prevent applications from turning into full-blown FISA surveillance applications, which require sufficient facts to support a finding of probable cause. Why is this important? By removing the presumption, the court may require officials to do additional investigation or provide more facts before obtaining the business records order from the court. This is problematic because section 215 authorities are most often used at the beginning of an investigation—thus, the simple relevance standard. At the beginning stages, it may be impossible or unduly burdensome to get the extra required information. As a result, this increased burden may inadvertently cause a potential lead in a national security investigation to be abandoned or critical terrorism links to be ignored.

Similarly, the new proof language will also cause delays in drafting applications as the government will no longer be able to rely on the presumption of relevance. As noted below, the 215 application process already suffers from inexcusable delays. Losing the presumption means the application itself will also be longer, as more and more information must be included. As we continue this fight against terrorism, we must ask ourselves a fundamental question: do we want our intelligence agents to spend more time doing paperwork or be out tracking terrorists?

Even more troubling than the potential administrative delays, the new proof language is amorphous and brand new in the national security context. By establishing a FISA court in the first place, Congress sought to create an environment in which national security matters would be handled by a specific pool of judges, thereby leading to greater certainty in how national security matters would be resolved by the courts. By injecting vague language into a statute that depends heavily on its definitions, it is likely that judges will have very different ideas about what constitutes "justif[ication]" of the applicant's belief of relevance. Our national security should not depend on an individual judge's interpretation of a term that has no analogous use in the entire FISA statute.

Lengthier applications employing vague and new legal standards will do nothing to improve the unreasonable delays in obtaining section 215 orders that were identified by the Department of Justice Inspector General in his March 2008 report. Remember, delays in acquiring basic information in a terrorism investigation can re-

[14] 50 U.S.C. § 1861(b)(2)(A) (2006).
[15] *Id.*

sult in the loss of intelligence, connections, and criminals, as well as a failure to "connect the dots" and prevent a terrorist attack. The 2008 Inspector General audit of section 215 usage identified considerable delays, up to several months, for processing routine business records applications in the Department of Justice. Given that it takes only hours to ordinarily obtain a grand jury subpoena, delays of this length are already unacceptable and must be addressed by the Department of Justice. It is likely, however, that this new amorphous language—rather than the clear, and well-understood, relevance standard—will simply worsen the problem.

2. Increases the Burden to Obtain Library Records from Third Parties

Despite the special exceptions and standards that already exist for obtaining library records under a section 215 court order,[16] S. 193 increases the standard to obtain library records that contain personally identifiable information about a library patron. Under S. 193, the government would have to present a statement of facts showing reasonable grounds to believe that tangible things are relevant to an authorized investigation *and* pertain to (a) an agent of a foreign power, (b) the activities of a suspected agent of a foreign power, or (c) an individual in contact with, or known to, a suspected agent of a foreign power subject to an authorized investigation. So, if the government could convince a court that there were reasonable grounds to believe that the business records sought were relevant to an authorized investigation, and if the government failed to show the involvement of a specific agent of a foreign power, then it would not be able to get the records. Such a requirement could disable the government from using a section 215 order at the early stages of an investigation, when such an order is most useful, simply because the government could not establish that the individual in question was an agent of a foreign power. Imposing this new requirement is an open invitation to terrorists to use unsuspecting third parties to communicate with associates on their behalf.

No special "library record" exception exists in the criminal law context. In fact, criminal investigators can obtain these records, without a court order, by obtaining a grand jury subpoena through a federal prosecutor. In the national security context, there is a special exception *plus* court authorization, both designed to protect civil liberties. In an interesting side note, the Department of Justice has pointed out that many libraries already take measures to inform their patrons that all records are erased every night to limit the disclosure of this information.

Enacting a separate and noticeably more stringent standard for library records will simply encourage terrorists to use library networks—either on their own or through unwitting third parties—to communicate with each other. It should come as no surprise that because of the heightened standards contained in the Leahy bill, it may be difficult for the national security investigators to quickly track such terrorists' usage of library computers.

[16] *See* 50 U.S.C. § 1861(a)(3) (2006).

3. For the First Time—Court Review of Business Records Minimization

S. 193 also requires FISA Court review of minimization procedures. Currently, section 215 requires that an application by the government include "an enumeration of the minimization procedures adopted" for business record orders. S. 193 would take this a step further and authorize the FISA Court to review and direct the government to follow the minimization procedures.

This additional requirement could lead to differing minimization requirements on each 215 order issued. It raises questions about how the FISA Court will view this new authority to direct the government to comply with minimization. Will the FISA Court require additional documentation, reporting, or other compliance measures under this new provision? How in depth will each federal judge require the minimization? This could lead to potential confusion among operational entities as they are ordered to impose different minimization procedures on essentially the same information within the same office because different judges proposed different minimization procedures. This could lead to operational uncertainty within offices hindering the ability to utilize leads obtained as a result of section 215 orders. Further, it poses potential compliance problems for offices that confuse minimization procedures among different collections of section 215 derived information resulting in potential sanctions on the government investigators by a federal judge or inspector general.

4. Immediate and Unlimited Judicial Review of Nondisclosure Orders

S. 193 allows recipients of section 215 orders and National Security Letters (NSLs) to challenge a nondisclosure requirement immediately and without end. This will require tasking investigative agencies and Department lawyers with defending nondisclosure orders much more often, possibly from the earliest moments of the investigation. In addition, since there is no limit, the recipient can challenge a non-disclosure order repeatedly until he succeeds. In most national security investigations, the ability to rule-in or rule-out certain information as being relevant to an investigation increases with time, as more facts are learned. Early in an investigation, it is not always readily apparent that a particular number that is the subject of a particular NSL is no longer relevant or that its disclosure will not cause any harm. This provision raises the risk that the FBI will be compelled to disclose the existence of an NSL or section 215 order, simply because the necessity for secrecy is often not provable until some time has elapsed, and the true value of the material becomes clear.

S. 193 Expands Burdens on Other Tools

On top of the additional restrictions S. 193 places on the expiring provisions, S. 193 alters three other criminal and intelligence tools that are not subject to sunset: FISA pen registers and trap and trace devices, NSLs, and delayed notice search warrants.

1. FISA Pen Registers/Trap and Trace Devices

A. Raises the Standard for FISA Pen Registers/Trap and Trace Devices

Pen registers (which retain a list of phone numbers called) and trap and trace devices (which catalogue a list of received calls) have long been used by law enforcement to obtain telephone transaction records. These devices do not capture the content of communications, just the source or destination of calls.[17] The Supreme Court has held that pen registers do not constitute a search under the Fourth Amendment and do not require a warrant because the individual "voluntarily conveyed numerical information to the telephone company."[18] Current law allows law enforcement to obtain pen registers and trap and trace devices from a judge under both criminal law and foreign intelligence surveillance law.[19] The standard to obtain pen registers and trap and trace devices is currently the same in these areas: that the information likely to be obtained is relevant.[20]

S. 193 would impose, for the first time ever, a higher requirement in the national security area, requiring the government's application to include "a statement of the facts and circumstances relied upon by the applicant to justify the belief of the applicant."[21] This new requirement replaces the current certification of relevance which has guided the use of FISA pen registers since their inception, and which mirrors the standard practice used in criminal investigations. As with many of the other tools impacted by the Leahy bill, pen registers are building blocks of an investigation. The simple requirement to certify the relevance of the information reflects the fact that early in an investigation, there may not be large amounts of information known or available to intelligence agents. For this reason, content may not be obtained through a pen register. This change in S. 193 destroys the parity between criminal and national security pen registers. Interestingly, it also creates the dynamic in which a spy, terrorist, or non-U.S. person could actually be given more protections than a U.S. person being investigated for an ordinary crime. This is a seismic shift in current law and sends the wrong signal to our agents in the field, by conveying that they must jump through more hoops in order to catch terrorists than ordinary criminals. Further, by making it more difficult for investigators to obtain pen registers in the counter-intelligence and counter-terrorism field than compared to traditional criminal law, it is a step further toward reconstituting the "wall" between criminal and national security investigations that the 9/11 Commission criticized, and the Committee followed through in knocking down.

B. Pen Register/Trap and Trace Minimization Required

S. 193 imposes a new requirement for minimization procedures to be applied to information obtained from FISA pen registers.

---

[17] *Smith* v. *Maryland*, 442 U.S. 735 (1979).
[18] *Id.*
[19] *Compare* 18 U.S.C. § 3122 (2006), *with* 50 U.S.C. § 1842 (2006).
[20] *Compare* 18 U.S.C. § 3122(b)(2) (2006), *with* 50 U.S.C. § 1842(c)(2) (2006).
[21] USA PATRIOT Act Sunset Extension Act of 2011, S. 193, 112th Cong. § 4 (2011).

Minimization is a concept ordinarily applied to the content of communications. This requirement raises questions about how minimization of non-content information is to be accomplished; what privacy interests are involved that may require minimization; and why this provision is even necessary. While proponents of S. 193 have claimed that they do not expect many substantive changes to current practice, it is highly likely that the FISA Court will interpret any change in law to mean that more procedures are necessary. This interpretation will lead to considerable operational confusion as both the court and agents/analysts struggle to apply minimization procedures, designed to protect U.S. person information, to data that is not readily identifiable as being U.S. person information. The irony is that imposing these procedures on dialing data, for example, will require that the FBI actually take a closer look at each number dialed to determine whether or not that number belongs to a U.S. person, effectively requiring agents to make an inquiry more invasive than current practice.

2. National Security Letters

A. Raises the Standard for Issuing a National Security Letter

S. 193 imposes a new requirement on investigators who wish to utilize NSLs, in effect making it even more difficult for federal authorities to investigate national security threats than to pursue common crimes like health care fraud, mail fraud, and tax evasion. Under S. 193, in addition to certifying relevance to a terrorist or intelligence investigation, investigators would also have to show "specific facts showing that there are reasonable grounds to believe that the information sought is relevant."[22] Such a standard is both vague and possibly difficult to meet in the early stages of investigation when NSLs are most useful.

This statement of "specific facts" is a holdover from negotiations following the Committee mark-up of S. 1692 in the last Congress. That bill originally included a provision requiring a "statement of specific and articulable facts." There was a debate surrounding this requirement and ultimately the term "articulable" was dropped. However, there was no further debate about what is, and is not, a "specific" fact.

Absent a definition of what makes a fact "specific", this new requirement has the potential to create confusion and compliance issues within the FBI. The cannons of statutory construction instruct judges that words in a statute have meanings, and that adding or removing words will have consequences in how those judges interpret the statute. Director Mueller agreed with this principle when he stated on March 16, 2011 that adding a new word to a statute can cause confusion and can put it "into a different ballpark."

This new standard could cause operational problems as well. For example, prior to 9/11 there was significant confusion about what was necessary to establish probable cause to obtain a FISA warrant to search the belongings of Zacharias Moussaoui, the "20th hijacker" on 9/11. FBI Special Agent Colleen Rowley testified before

[22] *Id.* at § 7 (2011).

this Committee in 2002 about the threshold necessary to establish probable cause. That testimony highlighted problems within the FBI in determining what standard applied to find probable cause. If the FBI had such a hard time determining what "probable cause" was, a basic standard in criminal investigations, how is the FBI going to interpret an undefined term like "specific", or will they experience the same paralyzing confusion with NSLs?

Further, this undefined requirement could lead to compliance problems with the Inspector General. Under current law, NSLs may be approved by a Special Agent in Charge of a FBI field office.[23] What if the Special Agent in Charge of the FBI's Chicago Field Office has a different opinion of what constitutes a "specific" fact than the Special Agent in Charge of the FBI's Miami Field Office? When the Inspector General for the Department of Justice starts auditing the issuance of National Security Letters, how do we know the Inspector General will not have a different idea of what "specific" means? It is entirely possible that the Inspector General and the FBI could have different definitions of what demonstrates a "specific" fact. FBI Director Mueller stated as much on March 16, 2011, when he said that there is a possibility that the Inspector General may have a different interpretation of whether specific facts were specific enough. This term, absent a definition, could unnecessarily cause confusion for the FBI in trying to figure out the difference between what constitutes a "specific" fact and what is just a fact.

B. Adds a new Sunset of National Security Letters

NSLs are a valuable tool and have provided investigators and analysts with critical information. Although details on NSL use are classified, the Justice Department has reported that "information obtained through NSLs has significantly advanced numerous sensitive terrorism and espionage investigations and has assisted the FBI in discovering links to previously unknown terrorist operatives." In its March 2007 report on NSLs, the Department of Justice Inspector General noted that "[m]any FBI personnel used terms to describe NSLs such as 'indispensable' or 'our bread and butter.'" As Valerie Caproni, General Counsel of the FBI, explained in 2007, "NSLs have been instrumental in breaking up cells like the 'Lackawanna Six' and the 'Northern Virginia Jihad.' Through the use of NSLs, the FBI has traced sources of terrorist funding, established telephone linkages that resulted in further investigation and arrests, and arrested suspicious associates with deadly weapons and explosives. NSLs allow the FBI to link terrorists together financially, and pinpoint cells and operatives by following the money."[24]

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

[23] *See* 18 U.S.C. § 2709(b) (2006).

[24] Hearing on: The Inspector General's Independent Report on the F.B.I.'s Use of National Security Letters: Hearing Before H. Comm. on the Judiciary, 110th Cong. (March 20, 2007) (statement of FBI General Counsel Valerie E. Caproni).

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. Under Section 505 of the PATRIOT Act, the FBI can use NSLs to obtain specified records so long as they 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 of the Constitution of the United States."

This protection ensures that NSLs may not be used for improper purposes. Although some deficiencies were found by the Department of Justice Inspector General concerning the FBI's handling of NSLs, the FBI and Department of Justice have responded to these findings and taken action to ensure that they are not repeated. In its March 2008 report on NSLs, the Inspector General stated that "the FBI and the Department have made significant progress in implementing the recommendations from [a prior Inspector General] report and in adopting other corrective actions to address serious problems we identified in the use of national security letters." What is puzzling is that the supposed remedy in S. 193—sunsetting the NSL standard to pre-September 11, 2001—generally has no relationship whatsoever to the deficiencies related to NSLs found by the Inspector General. In support, FBI Director Mueller affirmatively stated on March 16, 2011, that he is against a sunset for NSLs and does not support reverting to pre-9/11 standards.[25]

3. Shorter Time for Use of Delayed Notice Search Warrants

Delayed notice search warrants, well-accepted criminal investigative tools, allow investigators who have a court order to search a property without immediately informing the suspect.[26] S. 193 would dramatically and arbitrarily cut the time by which investigators must inform the suspect from 30 days to 7 days—less than a quarter of the time allowed under current law. In this instance, it would place this new burden on both national security and criminal investigations.

While it is true that applicants for a delayed notice search warrant may apply for an extension, up to 90 days or less, unless the facts of the case justify a longer delay, this requirement effectively takes law enforcement agents off the street in order to complete the required paperwork seeking the extension. The new disclosure requirements, if adopted, will force investigators to return to the

[25] Oversight Hearing on the Federal Bureau of Investigation: Before the H. Comm. on the Judiciary, 112th Cong. (2011) (response to Member questions by FBI Director Robert S. Mueller, III).

[26] *See* 18 U.S.C. § 3103a (2006).

issuing judge less than a week after they first received the warrant, and in some cases, before they have even had an opportunity to examine the material obtained. Investigators should be spending their time bringing offenders to justice, not at the courthouse deluging courts with unnecessary paperwork. It is also likely that courts will interpret this reduction by Congress as indicating that Congress frowns on delays of 30 days or more. This interpretation will make it harder for the government to obtain extensions beyond 30 days, much less up to 90. FBI Director Mueller stated that the 30-day delayed notice limitation works well and that there is no advantage to going back to 7 days.[27]

Additional Problems Created by Amendments Adopted

As part of the Committee's considerations of S. 193, Senators Leahy and Durbin offered amendments that further decrease the value and usefulness of critical national security tools. The Committee first adopted an amendment offered by Senator Leahy that would expand the list of business records that required additional scrutiny by the FISA court to include "bookseller records".

1. Leahy Amendment Regarding "Bookseller Records"

Currently, section 215 of the PATRIOT Act authorizes a national security investigator to make an application to the FISA Court for an order to require the production of "tangible things" including books, records, papers, documents, and other items. There are certain requirements that this application must satisfy and current applications can be quite lengthy. There is often a considerable delay, between three to six months, in obtaining a 215 order because of the multiple layers of review and approval a request goes through.

For the first time, the 2005 reauthorization of the PATRIOT Act created additional requirements for obtaining library circulation records, library patrol lists, book sales records, book customer lists, and certain other records (medical, firearm, and tax records). The 2005 amendment requires the FBI Director, or a high level designee, to approve the request before a court order is sought, as well as mandating specific congressional reporting. In contrast, library records can be obtained in criminal investigations with a grand jury subpoena, which does not require FBI Director approval or a court order.

In addition to the current carve-out for library and other records in the 2005 reauthorization, and the additional burdens to obtain library records contained in S. 193, this amendment further restricts national security investigators by expanding the exception to include "bookseller records." This amendment increases the burden on the government when obtaining business records from booksellers by putting commercial booksellers on the same level as public libraries.

The amendment defines bookseller records to include records reflecting the purchase or rental of "books, journals, or magazines, whether in digital form or in print." Exempting these records is problematic and creates an easily exploitable loophole for terrorists.

[27] Oversight Hearing on the Federal Bureau of Investigation, supra note 22.

Specifically, the amendment states that if the records sought contain bookseller records, the entire request rises to the new additional requirements. This special exception advertises to terrorists that they can increase the work of law enforcement simply by buying a book, or even better, obstruct investigators from even finding out about their activities by buying a magazine.

The recent arrest in Texas of Khalid Aldawsari highlights the severe limitations this amendment would put on law enforcement to prevent a terrorist attack. Aldawsari is a Saudi national who was attending college in Texas on a student visa. He was recently arrested and indicted for attempting to use a weapon of mass destruction. Fortunately, federal agents were able to prevent the terrorist attack, instead of cleaning up after it. To prevent this massive attack, an order was obtained under the section 215 business record authority, as confirmed by Robert S. Litt, General Counsel for the Director of National Intelligence.[28]

If the "bookseller records" amendment were the law this month when Aldawsari was investigated and arrested, it is possible that evidence of his bomb-making would not be obtainable with a section 215 order. According to the affidavit supporting the arrest of Aldawsari, he obtained many of the materials needed to build his weapon of mass destruction through online retailer Amazon.com—a bookseller. Through the use of a section 215 order, the FBI learned that this bookseller had records that include items Aldawsari purchased to build his bomb, including:

- three gallons of concentrated sulfuric acid;
- soldering iron;
- Christmas lights (wire for explosives and electronic circuits for improvised explosive devices);
- 3.2 million volt Stun Gun with built in flashlight;
- battery tester;
- alarm clock;
- precision screw driver set;
- chemistry flask;
- chemistry laboratory equipment set; and
- narrow mouth flask and 12″ glass stirring rod.[29]

These tangible things purchased are not books, journals, or magazines. They are components for making bombs. This amendment would essentially make online booksellers a refuge for terrorists, allowing them to acquire all their bomb-making supplies, while investigators are further handcuffed by the increased standards to obtain records from a third party. If this amendment had been the law, records about all of these purchases may have been held to the heightened standard as it is unclear how the FISA Court would treat an application for these records, merely because they came from a bookseller. Taken a step further, if Aldawsari had simply purchased a book with these items, it would have automatically triggered the heightened standard because the request would now include "bookseller records" as defined by the Leahy amendment.

As a practical matter, how would the investigators know if the records they were seeking included a book? It is likely that early

[28] USA PATRIOT Act Reauthorization, supra note 5.

[29] Federal Bureau of Investigation Aff. in Support of Criminal Complaint and Arrest Warrant for Khalid Aldawsari (February 23, 2011).

in an investigation, government agents would not know exactly what type of products were purchased and what records a 215 order will produce. For example, what if investigators knew Aldawsari was purchasing items from Amazon.com, but did not know what he was purchasing? Would the FISA Court automatically apply the heightened standard simply because Amazon.com is an online bookseller and FBI agents were unclear if the request would return "bookseller records"?

It is inconsistent for Congress to applaud the good work of investigators in preventing Aldawsari's terrorist attack while simultaneously creating laws that preclude investigators from utilizing those same tools when attempting to prevent the next attempted terrorist attack. By increasing the burdens required to obtain a section 215 order for both library and bookseller records, the application of this valuable tool could be rendered less effective in future investigations.

Aldawsari made other purchases from retailers that could be considered booksellers. For example, he made purchases from online retailer eBay, including a "Hazmat Suit Tychem BR Chemical Protective Clothing" and he failed to win an online auction for a "US M42 Gas Mask".[30] The tangible things Aldawsari purchased are not books, journals, or magazines. They are components for making bombs and protective gear from those hazardous materials. This amendment would essentially make online booksellers a refuge for terrorists, allowing them to acquire all of their bomb-making supplies, while investigators are further handcuffed by the increased standards to obtain records from a third party.

The Inspector General for the Department of Justice has already reported that FBI agents encountered processing delays for section 215 applications—averaging 147 days.[31] 147 days is an eternity in fast-moving operational situations. Adding new requirements, as the Leahy bill and amendment would do for libraries and booksellers, will only extend that delay. Ironically, these same records, potentially protected by the "bookseller records" amendment, are available in a matter of hours under a criminal grand jury subpoena. But in national security investigations, a grand jury subpoena is infrequently an option due to the need to keep national security concerns and interests classified.

2. Durbin Amendment Regarding John Doe Roving Wiretaps

Senator Durbin offered an amendment that was adopted by the Committee. His amendment inserted a particularity requirement into one of the specifications that must be made in a FISA electronic surveillance court order whenever the identity of the target of surveillance is not known. The stated purpose of the Durbin amendment was to require particularity for "John Doe" roving wiretaps. Unfortunately, this purpose was little more than a solution in search of a nonexistent problem.

Under current law, FISA allows the issuance of a wiretap against an individual in situations where the identity of the individual may not be known, but the government can describe the surveillance

[30] *Id.*
[31] U.S. Dep't of Justice, Office of the Inspector Gen., supra note 3.

target sufficiently to establish probable cause that he is an agent of a foreign power; this is a form of surveillance that has been labeled as a "John Doe" wiretap or search in the criminal context.

A challenge separate and distinct from the "John Doe" issue is presented when a surveillance target is taking measures to evade electronic surveillance. In such cases, section 206 of the USA PATRIOT Act allows the government to seek a "roving" court order when it can show that an individual is taking actions to "thwart" surveillance.[32] This roving order allows the government to continue its surveillance of the target as he switches from communication device to communication device without having to go back to the Foreign Intelligence Surveillance Court for a new court order. Unlike the "John Doe" situation where the identity of the target is not known, the problem in the roving context is that the government is initially unable to identify the communications facilities that the target is using now or in the future. Under section 105(c)(1)(B), the government may still obtain a FISA warrant when the facilities cannot be identified initially; however, in these situations, the government is required to provide notice to the Foreign Intelligence Surveillance Court within ten days after the date on which surveillance is initiated against any new facility or place.[33] This notice requirement is applicable in all "roving" situations.

Given these requirements for a roving wiretap court order, it is difficult to envision a real-life situation in which the government could successfully demonstrate that the target of the surveillance is attempting to evade surveillance without knowing the actual identity of the target—hence, the nonexistent problem of the "John Doe" roving wiretap "solution." Regardless, if the Durbin amendment was truly intended to amend FISA roving authority, then it should have amended the text in section 105(c)(2)(B)[34] where the roving authority is actually found. Instead, the Durbin amendment modified section 105(c)(1)(A)[35] which applies to all FISA electronic surveillance orders. If the Durbin amendment were to become law, the government would be required to describe the target with particularity in situations in which the identity of the target is unknown. This injects a new level of uncertainty into the FISA application and court order process as the Department of Justice and the Foreign Intelligence Surveillance Court attempt to interpret the effect and meaning of this new requirement. It is reasonable to assume that the Foreign Intelligence Surveillance Court will interpret this "particularity" standard to require a greater factual showing than is required under the present "description" standard. This could result in a delay or interruption of real-world intelligence operations and a corresponding loss of potential foreign intelligence information. Unlike the underlying Leahy bill, which the administration has at least grudgingly stated it "could live with," this Durbin amendment was not vetted with the Intelligence Community or the Department of Justice.

There has never been any allegation of abuse with respect to the use of the FISA "if known" standard in section 105(c)(1)(A). The

[32] 50 U.S.C. § 1805(c)(2)(B) (2006).
[33] 50 U.S.C. § 1805(c)(3) (2006).
[34] 50 U.S.C. § 1805(c)(2)(B) (2006).
[35] 50 U.S.C. § 1805(c)(1)(A) (2006).

provision has been working well since FISA's original enactment in 1978. In these limited situations in which the target's identity is unknown, the government is still required to provide, and the court must specify, a description of the target that satisfies the agent of a foreign power probable cause standard. The Constitutional "particularity" requirement is designed to prevent the use of a "general" warrant and to limit the scope of an actual physical search, e.g., if the warrant authorizes law enforcement to search for stolen televisions, then they are not permitted to search in desk drawers. The requirement for a "description" of the surveillance target prevents the FISA court order from becoming a general warrant and provides enough information to ensure that surveillance is conducted against the intended target.

It is important to remember that all FISA wiretaps, even John Doe and roving wiretaps, are ordered by a judge after the Attorney General has approved the request and the court has found probable cause that the surveillance target in question is a foreign power or an agent of a foreign power. The concept of a "John Doe roving wiretap" appears to be little more than a theoretical joining of two distinct statutory requirements in a combination not reflected by the reality of actual intelligence operations. This amendment, either as intended or drafted, is simply a solution in search of a problem.

3. Whitehouse Amendment Striking "and articulable"

Under current law, the government is only required to certify that records sought from a National Security Letter are relevant to an ongoing investigation. S. 193 would raise the standard for obtaining a National Security Letter by requiring the government to retain a written statement of "specific facts showing that there are reasonable grounds to believe that the information sought is relevant to the authorized investigation."

One section of S. 193 retained a version of this language that was a holdover from last Congress, requiring a "statement of specific and articulable facts" for an application for a nondisclosure order accompanying a NSL. The "specific and articulable" standards was included in S. 1692 during the previous Congress.[36] Subsequent negotiations modified this language to "specific facts" as incorporated into S. 193. As such, Senator Whitehouse's amendment was adopted by a voice vote. While we agree with the inclusion of this amendment for consistency in the bill, we disagree with the final language that now requires a statement of "specific facts".

Conclusion

Following September 11, 2001, Congress took steps to ensure that national security investigators had access to tools analogous to those long available to criminal investigators. The FBI has stated repeatedly that these tools have been critical in keeping the nation safe in the years since. Those who seek to weaken the tools currently available to our law enforcement and intelligence agencies must make the case that the existing law is unnecessary, counterproductive, or has been abused. No such case has been made. The

[36] The USA PATRIOT Act Sunset Extension Act of 2009, supra note 4.

Senate should act to make sure our law enforcement and intelligence professionals have the tools they need to stop those threats to our national security at every turn.

Despite the Majority's view that the classified member briefing revealed that S. 193 "poses no operational concerns," the Administration's stance has been only that they can "live with" the changes contained in S. 193. Being able to "live with" something is far different than having no concerns or supporting it. Interestingly, we have yet to hear anyone in the Administration say that S. 193 will actually help them keep this country safe. Moreover, the non-partisan members of the Federal Law Enforcement Agents Association, who operate independently of political considerations, oppose changes to the PATRIOT Act and said: "We would caution the Congress to be careful when trying to re-work any provisions that have already been in effect and have been effective."[37] While the Administration may be able to "live with" the changes contained in S. 193, we are concerned that in legislating distinct differences between national security and criminal laws this Committee is headed down a path that would rebuild the wall between national security and criminal cases. We all remember the tragic events of 9/11 and the serious work in Congress to implement the 9/11 Commission recommendations and tear down the wall between national security and criminal cases.

We continue to face threats from terrorists that originate abroad and at home. We have heard of no abuses of the existing authorities set to expire, but yet this legislation imposes a new set of burdens on law enforcement and national security investigators. Limiting the important investigative tools that have helped to thwart numerous terrorist attacks, by unnecessarily adding conditions to their already highly-regulated use, is a short-sighted strategy. As recent arrests and indictments demonstrate, these vital tools are being used responsibly and wisely by law enforcement and intelligence professionals to protect our nation from another terrorist attack. Now is definitely not the time for Congress to add new legal standards and bureaucratic requirements to the legal authorities our counterterrorism officials rely upon to identify and stop those responsible for planning these terror attacks.

We vigorously oppose the changes contained in S. 193 and, should it come before the full Senate, we will offer a number of amendments to limit the damage it would cause to critical national security and criminal law tools. Absent significant amendments to correct the problems we have highlighted, the Senate should reject S. 193 and extend the PATRIOT ACT without changes to current law.

CHARLES E. GRASSLEY.
ORRIN G. HATCH.
JON KYL.
JEFF SESSIONS.
LINDSEY GRAHAM.
JOHN CORNYN.
TOM COBURN.

---

[37] Letter from Jon Adler, National President, Federal Law Enforcement Officers Association, to Senator Patrick Leahy and Senator Charles Grassley, Senate Committee on the Judiciary (March 2, 2011) (on file with minority staff).

ADDITIONAL MINORITY VIEWS FROM SENATORS GRASSLEY, HATCH, KYL, SESSIONS, GRAHAM, AND CORNYN

EXPIRING PROVISIONS SHOULD BE MADE PERMANENT

On January 28, 2011, Attorney General Eric Holder and Director of National Intelligence James Clapper wrote to Speaker of the House Boehner, Majority Leader Reid, Minority Leader Pelosi, and Minority Leader McConnell. In that letter, Attorney General Holder and Director Clapper wrote, "In the current threat environment, it is imperative that our intelligence and law enforcement agencies have the tools they need to protect our national security."[1] The letter goes on to describe the importance of the three expiring provisions, including section 206 of the USA PATRIOT Act providing authority for roving surveillance, section 215 providing authority to compel production of business records and other tangible things, and section 6001 of the Intelligence Reform and Terrorism Prevention Act, otherwise known as the "lone wolf" provision, authorizing use of the Foreign Intelligence Surveillance Act (FISA) to target non-U.S. persons engaging in terrorism who are not associated with an identified terrorist group. The authors add, "*It is essential that these intelligence tools be reauthorized before they expire, and we are committed to working with Congress to ensure the speedy enactment of legislation to achieve this result*."[2]

In addition to this statement, where the emphasis was noted by the authors, they continued, "We also urge Congress to grant a reauthorization of sufficient duration to provide those charged with protecting our nation with the reasonable certainty and predictability. When Congress originally enacted the PATRIOT Act, it included a three-year sunset on these authorities. While we welcome Congressional oversight into the use of these tools, Congress did not contemplate that this sunset would devolve into a series of short-term extensions that increase the uncertainties borne by our intelligence and law enforcement agencies in carrying out their missions."[3] Despite this clear statement in support of reauthorizing the expiring authorities, we are now, two months later, addressing yet another short term extension extending the PATRIOT Act provisions set to expire now on May 27, 2011.[4]

Notwithstanding the calls from the Attorney General and Director Clapper, S. 193 would simply extend the expiring provisions until December 2013, just 33 months from now. By extending the three provisions for a short term, albeit nearly three years, Congress fails to provide needed certainty to law enforcement and counterterrorism officials. In fact, Director of the Federal Bureau

---

[1] Letter from Director of National Intelligence James R. Clapper and Attorney General Eric Holder to House Speaker John Boehner, Senate Majority Leader Harry Reid, House Minority Leader Nancy Pelosi, and Senate Minority Leader McConnell (Jan. 28, 2011) (on file with minority staff).

[2] *Id.* (emphasis in original).

[3] *Id.*

[4] FISA Sunsets Extension Act of 2011, Pub. L. No. 112–3, 125 Stat. 5 (2011).

of Investigation (FBI) Robert Mueller III testified before the Senate Select Committee on Intelligence on February 16, 2011, that the expiring provisions were critical to ongoing investigations and should be permanently reauthorized.[5] Similarly, the Federal Law Enforcement Officers Association (FLEOA), a non-profit law enforcement association representing over 26,000 federal law enforcement officers, wrote to Senate Minority Leader McConnell on February 7, 2011, supporting "legislation that seeks to incorporate a long-term solution to the USA PATRIOT Act's problematic recurring expiration date."[6] The letter added, "Crime and terrorism will not "sunset" and terrorists don't need any "extension" to continue their heinous activities. Just like handcuffs, this tool should be a permanent part of the law enforcement arsenal. Arguments to the contrary are flawed and don't recognize the reality that the Act has been judiciously used and has kept Americans safe . . . Terrorists don't "sunset" and the tools needed to stop them shouldn't either."[7] A subsequent letter from FLEOA to members of the Judiciary Committee dated March 2, 2011, added, "We would caution the Congress to be careful when trying to re-work any provisions that have already been in effect and have been effective. Additionally, the short-term authorization is at odds with a Congress that in the aftermath of September 11th, 2001 attacks asked "Why didn't we know and connect the dots? The USA PATRIOT Act removed some of the barriers in place that prevented us from "connecting the dots" and any retraction of those provisions is in effect, "re-building the wall."[8]

We wholeheartedly agree with FLEOA and the federal agents on the ground that the organization represents. The terrorist threat is not going away anytime soon and efforts to continually renew these provisions on an ad hoc basis provide little, if any, operational certainty to agents in the field.

Continuing to temporarily postpone sunsets of these critical national security tools runs the risk that eventually the sunsets will be allowed to lapse, causing operational problems. Further, in continually reauthorizing these expiring sunsets, we in Congress continue to amend the provisions making them more difficult to use with so many requirements that they become unduly burdensome and functionally useless. Despite erroneous statements to the contrary, the three expiring provisions have not been the subject of abuse. In the case of section 215 orders, the Inspector General of the Department of Justice has twice reviewed the use of the authority and "did not identify *any* illegal use of Section 215 authority."[9] In fact, Section 215 orders are crucial to the early stages of a terrorism investigation, allowing the government to obtain information at an early investigative stage, helping to connect dots.

---

[5] Chris Strohm, PATRIOT Act Extension Enters Home Stretch, NAT'L JOURNAL, Feb. 16, 2011, available at http://www.nationaljournal.com/nationalsecurity/patriot-act-extension-enters-home-stretch–20110216?mrefid=site1search.

[6] Letter from Jon Adler, National President, Federal Law Enforcement Officers Association, to Minority Leader Mitch McConnell, United States Senate (Feb. 7, 2011) (on file with minority staff).

[7] *Id.*

[8] Letter from Jon Adler, National President, Federal Law Enforcement Officers Association, to Senator Patrick Leahy and Senator Charles Grassley, Senate Committee on the Judiciary (March 2, 2011) (on file with minority staff).

[9] Office of the Inspector Gen., U.S. Dep't of Justice, A Review of the FBI's Use of Section 215 Orders for Business Records in 2006 at 5 (March 2008) (emphasis added).

This vital tool has become a staple of counterterrorism efforts, with investigators utilizing this authority 223 times between 2004 and 2007.[10] FBI Director Mueller has called this tool "exceptionally helpful and useful in our national security investigations."[11]

Similarly, section 6001 of the Intelligence Reform and Terrorism Protection Act, known as the "lone wolf" provision, has not ever been used, much less abused. However, the absence of utilization does not provide support as some have argued to call for its expiration. For example, FBI Director Mueller, Secretary of Homeland Security Napolitano, and Attorney General Holder have all raised concerns that the current threat environment has evolved with the development and proliferation of self-radicalized, home grown terrorists. This is precisely the scenario the lone wolf provision was designed to help thwart. In fact, a September 14, 2009, letter from Assistant Attorney General Ron Weich stated, "the prospect of a terrorist who 'self-radicalizes' by means of information and training provided by a variety of international terrorist groups via the internet"[12] is one possible scenario the lone wolf provision would help protect against.

Finally, section 206 authorizing the roving surveillance authority is also without reported abuses. In fact, in recent testimony before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security, the General Counsel for the Office of Director of National Intelligence provided a specific example of how the provision is being utilized to track a foreign agent who "changes cellular phones frequently."[13]

These three provisions have provided law enforcement and national security investigators the vital tools necessary to investigate a host of terrorism cases. If we simply kick the can down the road and delay the sunset of these provisions we risk losing the operational edge against an enemy that have proven to be methodical and resilient. Failing to recognize that our enemy continues to watch our every move and adjust their operational readiness to match the changes we make to our counterterrorism tools would be a significant miscalculation. We must show those who seek to harm our citizens and our way of life that we are willing to do what it takes to prevent them from waging attacks on our soil. Permanently extending the three expiring provisions would send such a signal and ensure the operational continuity that agents on the ground, at home and abroad, deserve.

CHARLES E. GRASSLEY.
ORRIN G. HATCH.
JON KYL.
JEFF SESSIONS.
LINDSEY GRAHAM.
JOHN CORNYN.

---

[10] Oversight of the Federal Bureau of Investigation: Hearing Before the S. Comm. On the Judiciary, 111th Cong. 24 (statement of Robert S. Mueller, III, Dir. Fed. Bureau of Investigation).

[11] *Id.*

[12] Letter from Assistant Attorney Gen. Ron Weich, U.S. Dep't of Justice, to Senator Patrick Leahy, Chairman, Sen. Comm. on the Judiciary (Sept. 14, 2009) (on file with minority staff).

[13] USA PATRIOT Act Reauthorization: Hearing Before the Subcomm. On Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary, 112th Cong. (March 9, 2011) (statement of Robert S. Litt, General Counsel, Office of the Dir. Of Nat'l Intelligence).

VIII. CHANGES TO EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by S. 193, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

UNITED STATES CODE

TITLE 12—BANKS AND BANKING

* * * * * * *

CHAPTER 35—RIGHT TO FINANCIAL PRIVACY

* * * * * * *

SEC. 3414. SPECIAL PROCEDURES.

(a)(1) Nothing in this chapter (except sections 3415, 3417, 3418, and 3421 of this title) shall apply to the production and disclosure of financial records pursuant to requests from—

(A) a Government authority authorized to conduct foreign counter- or foreign positive-intelligence activities for purposes of conducting such activities;

(B) the Secret Service for the purpose of conducting its protective functions (18 U.S.C. 3056; 18 U.S.C. 3056A, Public Law 90–331, as amended); or

(C) a Government authority authorized to conduct investigations of, or intelligence or counterintelligence analyses related to, international terrorism for the purpose of conducting such investigations or analyses.

(2) In the instances specified in paragraph (1), the Government authority shall submit to the financial institution the certificate required in section 3403(b) of this title signed by a supervisory official of a rank designated by the head of the Government authority.

(3)(A) If the Government authority described in paragraph (1) or the Secret Service, as the case may be, 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 Government authority or the Secret Service has sought or obtained access to a customer's financial records.

(B) The request shall notify the person or entity to whom the request is directed of the nondisclosure requirement under subparagraph (A).

(C) 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 subparagraph (A).

(D) At the request of the authorized Government authority or the Secret Service, any person making or intending to make a disclosure under this section shall identify to the requesting official of the authorized Government authority or the Secret Service 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 authorized Government authority or the Secret Service 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 this subsection.

(4) The Government authority specified in paragraph (1) shall compile an annual tabulation of the occasions in which this section was used.

(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 Director of the Federal Bureau of Investigation, or a 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 make a certification under subparagraph (A) only upon a written statement, which shall be retained by the Federal Bureau of Investigation, of specific facts showing that there are reasonable grounds to believe that the information sought is relevant to the authorized investigation described in subparagraph (A).

(C)¿(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.

(D)¿(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).

(E) PROHIBITION OF CERTAIN DISCLOSURE.—

(i) PROHIBITION.—

(I) IN GENERAL.—If a certification is issued under subclause(II) and notice of the right to judicial review under clause (iii) is provided, no financial institution, or officer, employee, or agent thereof, that receives a request under subparagraph (A), shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under subparagraph (A).

(II) CERTIFICATION.—The requirements of subclause (I) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office, certifies that, absent a prohibition of disclosure under this subparagraph, there may result—

(aa) a danger to the national security of the United States;

(bb) interference with a criminal, counterterrorism, or counterintelligence investigation;

(cc) interference with diplomatic relations; or

(dd) danger to the life or physical safety of any person.

(ii) EXCEPTION.—

(I) IN GENERAL.—A financial institution, or officer, employee, or agent thereof, that receives a request under subparagraph (A) may disclose information otherwise subject to any applicable nondisclosure requirement to—

(aa) those persons to whom disclosure is necessary in order to comply with the request;

(bb) an attorney in order to obtain legal advice or assistance regarding the request; or

(cc) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(II) PERSONS NECESSARY FOR COMPLIANCE.—Upon a request by the Director of the Federal Bureau of Investigation or the designee of the Director, those persons to whom disclosure will be made under subclause (I)(aa) or to whom such disclosure was made before the request shall be identified to the Director or the designee.

(III) NONDISCLOSURE REQUIREMENT.—A person to whom disclosure is made under subclause (I) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subparagraph (A) in the same manner as the person to whom the request is issued.

(IV) NOTICE.—Any recipient that discloses to a person described in subclause (I) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

(iii) RIGHT TO JUDICIAL REVIEW.—

(I) IN GENERAL.—A financial institution that receives a request under subparagraph (A) shall have the right to judicial review of any applicable nondisclosure requirement.

(II) NOTIFICATION.—A request under subparagraph (A) shall state that if the recipient wishes to have a court review a nondisclosure requirement, the recipient shall notify the Government.

(III) INITIATION OF PROCEEDINGS.—If a recipient of a request under subparagraph (A) makes a notification under subclause (II), the Government shall initiate judicial review under the procedures established in section 3511 of title 18, United States Code, unless an appropriate official of the Federal Bureau of Investigation makes a notification under clause (iv).

(iv) TERMINATION.—In the case of any request for which a financial institution has submitted a notification under clause (iii)(II), if the facts supporting a nondisclosure requirement cease to exist, an appropriate official of the Federal Bureau of Investigation shall promptly notify the financial institution, or officer, employee, or agent thereof, subject to the nondisclosure requirement that the nondisclosure requirement is no longer in effect.

(b)(1) Nothing in this chapter shall prohibit a Government authority from obtaining financial records from a financial institution

if the Government authority determines that delay in obtaining access to such records would create imminent danger of—

(A) physical injury to any person;

(B) serious property damage; or

(C) flight to avoid prosecution.

(2) In the instances specified in paragraph (1), the Government shall submit to the financial institution the certificate required in section 3403(b) of this title signed by a supervisory official of a rank designated by the head of the Government authority.

(3) Within five days of obtaining access to financial records under this subsection, the Government authority shall file with the appropriate court a signed, sworn statement of a supervisory official of a rank designated by the head of the Government authority setting forth the grounds for the emergency access. The Government authority shall thereafter comply with the notice provisions of section 3409(c) of this title.

(4) The Government authority specified in paragraph (1) shall compile an annual tabulation of the occasions in which this section was used.

(d) For purposes of this section, and sections 3415 and 3417 of this title insofar as they relate to the operation of this section, the term "financial institution" has the same meaning as in subsections (a)(2) and (c)(1) of section 5312 of Title 31, except that, for purposes of this section, such term shall include only such a financial institution any part of which is located inside any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, or the United States Virgin Islands.

* * * * * * *

TITLE 15—COMMERCE AND TRADE

* * * * * * *

CHAPTER 41—CONSUMER CREDIT PROTECTION

Subchapter III—Credit Reporting Agencies

SEC. 1681u. DISCLOSURES TO FBI FOR COUNTERINTELLIGENCE PURPOSES.

* * * * * * *

¿(d) CONFIDENTIALITY.—

¿(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 consumer reporting agency or officer, employee, or agent of a 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) that the Federal Bureau of Investigation has sought or obtained the identity of financial institutions or a consumer report respecting any consumer under subsection (a), (b), or (c) of this section, and no consumer reporting agency or officer, employee, or agent of a consumer reporting agency shall include in any consumer report any information that would indicate that the Federal Bureau of Investigation has sought or obtained such information on a consumer report.

¿(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 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 the identity of financial institutions or a consumer report respecting any consumer under this section.

(d) WRITTEN STATEMENT.—The Director of the Federal Bureau of Investigation, or a 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 make a certification under subsection (a) or (b) only upon a written statement, which shall be retained by the Federal Bureau of Investigation, of specific facts showing that there are reasonable grounds to believe that the information sought is relevant to the authorized investigation described in subsection (a) or (b), as the case may be.

(e) PROHIBITION OF CERTAIN DISCLOSURE.—

(1) PROHIBITION.—

(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under paragraph (3) is provided, no consumer reporting agency, or officer, employee, or agent thereof, that receives a request or order under subsection (a), (b), or (c), shall disclose or specify in any consumer report, that the Federal Bureau of Investigation has sought or obtained access to information or records under subsection (a), (b), or (c).

(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau

headquarters or a Special Agent in Charge of a Bureau field office, certifies that, absent a prohibition of disclosure under this subsection, there may result)—

(i) a danger to the national security of the United States;

(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

(iii) interference with diplomatic relations; or

(iv) danger to the life or physical safety of any person.

(2) EXCEPTION.—

(A) IN GENERAL.—A consumer reporting agency, or officer, employee, or agent thereof, that receives a request or order under subsection (a), (b), or (c) may disclose information otherwise subject to any applicable nondisclosure requirement to—

(i) those persons to whom disclosure is necessary in order to comply with the request or order;

(ii) an attorney in order to obtain legal advice or assistance regarding the request or order; or

(iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(B) PERSONS NECESSARY FOR COMPLIANCE.—Upon a request by the Director of the Federal Bureau of Investigation or the designee of the Director, those persons to whom disclosure will be made under subparagraph (A)(i) or to whom such disclosure was made before the request shall be identified to the Director or the designee.

(C) NONDISCLOSURE REQUIREMENT.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request or order is issued under subsection (a), (b), or (c) in the same manner as the person to whom the request or order is issued.

(D) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

(3) RIGHT TO JUDICIAL REVIEW.—

(A) IN GENERAL.—A consumer reporting agency that receives a request or order under subsection (a), (b), or (c) shall have the right to judicial review of any applicable nondisclosure requirement.

(B) NOTIFICATION.—A request or order under subsection (a), (b), or (c) shall state that if the recipient wishes to have a court review a nondisclosure requirement, the recipient shall notify the Government.

(C) INITIATION OF PROCEEDINGS.—If a recipient of a request or order under subsection (a), (b), or (c) makes a notification under subparagraph (B), the Government shall initiate judicial review under the procedures established in section 3511 of title 18, United States Code, unless an ap-

propriate official of the Federal Bureau of Investigation makes a notification under paragraph (4).

(4) TERMINATION.—In the case of any request or order for which a consumer reporting agency has submitted a notification under paragraph (3)(B), if the facts supporting a nondisclosure requirement cease to exist, an appropriate official of the Federal Bureau of Investigation shall promptly notify the consumer reporting agency, or officer, employee, or agent thereof, subject to the nondisclosure requirement that the nondisclosure requirement is no longer in effect.

(*f*)¿(e) PAYMENT OF FEES.—The Federal Bureau of Investigation shall, subject to the availability of appropriations, pay to the consumer reporting agency assembling or providing report or information in accordance with procedures established under this section a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching, reproducing, or transporting books, papers, records, or other data required or requested to be produced under this section.

(*g*)¿(f) LIMIT ON DISSEMINATION.—The Federal Bureau of Investigation may not disseminate information obtained pursuant to this section outside of the Federal Bureau of Investigation, except to other Federal agencies as may be necessary for the approval or conduct of a foreign counterintelligence investigation, or, where the information concerns a person subject to the Uniform Code of Military Justice, to appropriate investigative authorities within the military department concerned as may be necessary for the conduct of a joint foreign counterintelligence investigation.

(*h*)¿(g) RULES OF CONSTRUCTION.—Nothing in this section shall be construed to prohibit information from being furnished by the Federal Bureau of Investigation pursuant to a subpoena or court order, in connection with a judicial or administrative proceeding to enforce the provisions of this subchapter. Nothing in this section shall be construed to authorize or permit the withholding of information from the Congress.

(*i*)¿(h) REPORTS TO CONGRESS.—

(1) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence and the Committee on Banking, Finance and Urban Affairs of the House of Representatives, and the Select Committee on Intelligence and the Committee on Banking, Housing, and Urban Affairs of the Senate concerning all requests made pursuant to subsections (a), (b), and (c) 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.

(*j*)¿(i) DAMAGES.—Any agency or department of the United States obtaining or disclosing any consumer reports, records, or information contained therein in violation of this section is liable to the consumer to whom such consumer reports, records, or information relate in an amount equal to the sum of—

(1) $100, without regard to the volume of consumer reports, records, or information involved;

(2) any actual damages sustained by the consumer as a result of the disclosure;

(3) if the violation is found to have been willful or intentional, such punitive damages as a court may allow; and

(4) in the case of any successful action to enforce liability under this subsection, the costs of the action, together with reasonable attorney fees, as determined by the court.

(*k*)¿(j) DISCIPLINARY ACTIONS FOR VIOLATIONS.—If a court determines that any agency or department of the United States has violated any provision of this section and the court finds that the circumstances surrounding the violation raise questions of whether or not an officer or employee of the agency or department acted willfully or intentionally with respect to the violation, the agency or department shall promptly initiate a proceeding to determine whether or not disciplinary action is warranted against the officer or employee who was responsible for the violation.

(*l*)¿(k) GOOD-FAITH EXCEPTION.—Notwithstanding any other provision of this subchapter, any consumer reporting agency or agent or employee thereof making disclosure of consumer reports or identifying information pursuant to this subsection in good-faith reliance upon a certification of the Federal Bureau of Investigation pursuant to 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.

(*m*)¿(l) LIMITATION OF REMEDIES.—Notwithstanding any other provision of this subchapter, the remedies and sanctions set forth in this section shall be the only judicial remedies and sanctions for violation of this section.

(*n*)¿(m) INJUNCTIVE RELIEF.—In addition to any other remedy contained in this section, injunctive relief shall be available to require compliance with the procedures of this section. In the event of any successful action under this subsection, costs together with reasonable attorney fees, as determined by the court, may be recovered.

SEC. 1681v. DISCLOSURES TO GOVERNMENTAL AGENCIES FOR COUNTERTERRORISM PURPOSES

(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) *CERTIFICATION*.—¿FORM OF CERTIFICATION.—The certification

(1) 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.

(2) WRITTEN STATEMENT.—A supervisory official or officer described in paragraph (1) may make a certification under subsection (a) only upon a written statement, which shall be retained by the government agency, of specific facts showing that there are reasonable grounds to believe that the information sought is relevant to the authorized investigation described in subsection (a).

¿(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.

(c) PROHIBITION OF CERTAIN DISCLOSURE.—

(1) PROHIBITION.—

(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under paragraph (3) is provided, no consumer reporting agency, or officer, employee, or agent thereof, that receives a request under subsection (a), shall disclose to any person or specify in any consumer report, that a government agen-

cy has sought or obtained access to information under subsection (a).

(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the head of a government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism, or a designee, certifies that, absent a prohibition of disclosure under this subsection, there may result—

(i) a danger to the national security of the United States;

(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

(iii) interference with diplomatic relations; or

(iv) danger to the life or physical safety of any person.

(2) EXCEPTION.—

(A) IN GENERAL.—A consumer reporting agency, or officer, employee, or agent thereof, that receives a request under subsection (a) may disclose information otherwise subject to any applicable nondisclosure requirement to—

(i) those persons to whom disclosure is necessary in order to comply with the request;

(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

(iii) other persons as permitted by the head of the government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism, or a designee.

(B) PERSONS NECESSARY FOR COMPLIANCE.—Upon a request by the head of a government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism, or a designee, those persons to whom disclosure will be made under subparagraph (A)(i) or to whom such disclosure was made before the request shall be identified to the head of the government agency or the designee.

(C) NONDISCLOSURE REQUIREMENT.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (a) in the same manner as the person to whom the request is issued.

(D) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

(3) RIGHT TO JUDICIAL REVIEW.—

(A) IN GENERAL.—A consumer reporting agency that receives a request under subsection (a) shall have the right to judicial review of any applicable nondisclosure requirement.

(B) NOTIFICATION.—A request under subsection (a) shall state that if the recipient wishes to have a court review a

nondisclosure requirement, the recipient shall notify the government.

(C) INITIATION OF PROCEEDINGS.—If a recipient of a request under subsection (a) makes a notification under subparagraph (B), the government shall initiate judicial review under the procedures established in section 3511 of title 18, United States Code, unless an appropriate official of the government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism makes a notification under paragraph (4).

(4) TERMINATION.—In the case of any request for which a consumer reporting agency has submitted a notification under paragraph (3)(B), if the facts supporting a nondisclosure requirement cease to exist, an appropriate official of the government agency authorized to conduct investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism shall promptly notify the consumer reporting agency, or officer, employee, or agent thereof, subject to the nondisclosure requirement that the nondisclosure requirement is no longer in effect.

(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 [FN1], 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.

"(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).

"(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 507 of the National Security Act of 1947 (50 U.S.C. 415b).".

* * * * * * *

TITLE 18—CRIMES AND CRIMINAL PROCEDURE

PART I—CRIMES

CHAPTER 10—BIOLOGICAL WEAPONS

SEC. 175c. VARIOLA VIRUS.

(a) UNLAWFUL CONDUCT.—

(1) IN GENERAL.—Except as provided in paragraph (2), it shall be unlawful for any person to knowingly produce, engineer, synthesize, acquire, transfer directly or indirectly, receive, possess, import, export, or use, or possess and threaten to use, variola virus.

(2) EXCEPTION.—This subsection does not apply to conduct by, or under the authority of, the Secretary of Health and Human Services.

(b) JURISDICTION.—Conduct prohibited by subsection (a) is within the jurisdiction of the United States if—

(1) the offense occurs in or affects interstate or foreign commerce;

(2) the offense occurs outside of the United States and is committed by a national of the United States;

(3) the offense is committed against a national of the United States while the national is outside the United States;

(4) the offense is committed against any property that is owned, leased, or used by the United States or by any department or agency of the United States, whether the property is within or outside the United States; or

(5) an offender aids or abets any person over whom jurisdiction exists under this subsection in committing an offense under this section or conspires with any person over whom jurisdiction exists under this subsection to commit an offense under this section.

(c) CRIMINAL PENALTIES.—

(1) IN GENERAL.—Any person who violates, or attempts or conspires to violate, subsection (a) shall be fined not more than $2,000,000 and shall be sentenced to a term of imprisonment not less than 25 years or to imprisonment for life.

(2) OTHER CIRCUMSTANCES.—Any person who, in the course of a violation of subsection (a), uses, attempts or conspires to use, or possesses and threatens to use, any item or items described in subsection (a), shall be fined not more than $2,000,000 and imprisoned for not less than 30 years or imprisoned for life.

(3) SPECIAL CIRCUMSTANCES.—If the death of another results from a person's violation of subsection (a), the person shall be fined not more than $2,000,000 and punished by *death or* imprisonment for life.

(d) DEFINITION.—As used in this section, the term "variola virus" means a virus that can cause human smallpox or any derivative of the variola major virus that contains more than 85 percent of the gene sequence of the variola major virus or the variola minor virus.

* * * * * * *

CHAPTER 39—EXPLOSIVES AND OTHER DANGEROUS ARTICLES

SEC. 832. PARTICIPATION IN NUCLEAR AND WEAPONS OF MASS DESTRUCTION THREATS TO THE UNITED STATES.

(a) Whoever, within the United States or subject to the jurisdiction of the United States, willfully participates in or knowingly provides material support or resources (as defined in section 2339A) to a nuclear weapons program or other weapons of mass destruction program of a foreign terrorist power, or attempts or conspires to do so, shall be imprisoned for not more than 20 years.

(b) There is extraterritorial Federal jurisdiction over an offense under this section.

(c) Whoever without lawful authority develops, possesses, or attempts or conspires to develop or possess a radiological weapon, or threatens to use or uses a radiological weapon against any person within the United States, or a national of the United States while such national is outside of the United States or against any property that is owned, leased, funded, or used by the United States, whether that property is within or outside of the United States, shall be *punished by death if death results to any person from the offense, or* imprisoned for any term of years or for life.

(d) As used in this section—

(1) "nuclear weapons program" means a program or plan for the development, acquisition, or production of any nuclear weapon or weapons;

(2) "weapons of mass destruction program" means a program or plan for the development, acquisition, or production of any weapon or weapons of mass destruction (as defined in section 2332a(c));

(3) "foreign terrorist power" means a terrorist organization designated under section 219 of the Immigration and Nationality Act, or a state sponsor of terrorism designated under section 6(j) of the Export Administration Act of 1979 or section 620A of the Foreign Assistance Act of 1961; and

(4) "nuclear weapon" means any weapon that contains or uses nuclear material as defined in section 831(f)(1).

* * * * * * *

CHAPTER 113B—TERRORISM

SEC. 2332g. MISSILE SYSTEMS DESIGNED TO DESTROY AIRCRAFT.

(a) UNLAWFUL CONDUCT.—

(1) IN GENERAL.—Except as provided in paragraph (3), it shall be unlawful for any person to knowingly produce, construct, otherwise acquire, transfer directly or indirectly, receive, possess, import, export, or use, or possess and threaten to use—

(A) an explosive or incendiary rocket or missile that is guided by any system designed to enable the rocket or missile to—

(i) seek or proceed toward energy radiated or reflected from an aircraft or toward an image locating an aircraft; or

(ii) otherwise direct or guide the rocket or missile to an aircraft;

(B) any device designed or intended to launch or guide a rocket or missile described in subparagraph (A); or

(C) any part or combination of parts designed or redesigned for use in assembling or fabricating a rocket, missile, or device described in subparagraph (A) or (B).

(2) NONWEAPON.—Paragraph (1)(A) does not apply to any device that is neither designed nor redesigned for use as a weapon.

(3) EXCLUDED CONDUCT.—This subsection does not apply with respect to—

(A) conduct by or under the authority of the United States or any department or agency thereof or of a State or any department or agency thereof; or

(B) conduct pursuant to the terms of a contract with the United States or any department or agency thereof or with a State or any department or agency thereof.

(b) JURISDICTION.—Conduct prohibited by subsection (a) is within the jurisdiction of the United States if—

(1) the offense occurs in or affects interstate or foreign commerce;

(2) the offense occurs outside of the United States and is committed by a national of the United States;

(3) the offense is committed against a national of the United States while the national is outside the United States;

(4) the offense is committed against any property that is owned, leased, or used by the United States or by any department or agency of the United States, whether the property is within or outside the United States; or

(5) an offender aids or abets any person over whom jurisdiction exists under this subsection in committing an offense under this section or conspires with any person over whom jurisdiction exists under this subsection to commit an offense under this section.

(c) CRIMINAL PENALTIES.—

(1) IN GENERAL.—Any person who violates, or attempts or conspires to violate, subsection (a) shall be fined not more than $2,000,000 and shall be sentenced to a term of imprisonment not less than 25 years or to imprisonment for life.

(2) OTHER CIRCUMSTANCES.—Any person who, in the course of a violation of subsection (a), uses, attempts or conspires to use, or possesses and threatens to use, any item or items de-

scribed in subsection (a), shall be fined not more than $2,000,000 and imprisoned for not less than 30 years or imprisoned for life.

(3) SPECIAL CIRCUMSTANCES.—If the death of another results from a person's violation of subsection (a), the person shall be *punished by death or* fined not more than $2,000,000 and punished by imprisonment for life.

(d) DEFINITION.—As used in this section, the term ''aircraft'' has the definition set forth in section 40102(a)(6) of title 49, United States Code.

* * * * * * *

SEC. 2332h. RADIOLOGICAL DISPERSAL DEVICES.

(a) UNLAWFUL CONDUCT.—

(1) IN GENERAL.—Except as provided in paragraph (2), it shall be unlawful for any person to knowingly produce, construct, otherwise acquire, transfer directly or indirectly, receive, possess, import, export, or use, or possess and threaten to use—

(A) any weapon that is designed or intended to release radiation or radioactivity at a level dangerous to human life; or

(B) any device or other object that is capable of and designed or intended to endanger human life through the release of radiation or radioactivity.

(2) EXCEPTION.—This subsection does not apply with respect to—

(A) conduct by or under the authority of the United States or any department or agency thereof; or

(B) conduct pursuant to the terms of a contract with the United States or any department or agency thereof.

(b) JURISDICTION.—Conduct prohibited by subsection (a) is within the jurisdiction of the United States if—

(1) the offense occurs in or affects interstate or foreign commerce;

(2) the offense occurs outside of the United States and is committed by a national of the United States;

(3) the offense is committed against a national of the United States while the national is outside the United States;

(4) the offense is committed against any property that is owned, leased, or used by the United States or by any department or agency of the United States, whether the property is within or outside the United States; or

(5) an offender aids or abets any person over whom jurisdiction exists under this subsection in committing an offense under this section or conspires with any person over whom jurisdiction exists under this subsection to commit an offense under this section.

(c) CRIMINAL PENALTIES.—

(1) IN GENERAL.—Any person who violates, or attempts or conspires to violate, subsection (a) shall be fined not more than $2,000,000 and shall be sentenced to a term of imprisonment not less than 25 years or to imprisonment for life.

(2) OTHER CIRCUMSTANCES.—Any person who, in the course of a violation of subsection (a), uses, attempts or conspires to use, or possesses and threatens to use, any item or items described in subsection (a), shall be fined not more than $2,000,000 and imprisoned for not less than 30 years or imprisoned for life.

(3) SPECIAL CIRCUMSTANCES.—If the death of another results from a person's violation of subsection (a), the person shall be fined not more than $2,000,000 and punished by *death or* imprisonment for life.

* * * * * * *

CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

SEC. 2709. COUNTERINTELLIGENCE ACCESS TO TELEPHONE TOLL AND TRANSACTIONAL RECORDS.

(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, counter-

terrorism, 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).

(c) WRITTEN STATEMENT.—The Director of the Federal Bureau of Investigation, or a 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 make a certification under subsection (b) only upon a written statement, which shall be retained by the Federal Bureau of Investigation, of specific facts showing that there are reasonable grounds to believe that the information sought is relevant to the authorized investigation described in subsection (b).

(d) PROHIBITION OF CERTAIN DISCLOSURE.—

(1) PROHIBITION.—

(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under paragraph (3) is provided, no wire or electronic communication service provider, or officer, employee, or agent thereof, that receives a request under subsection (a), shall disclose to any person that the Director of the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the Director of the Federal Bureau of Investigation, or a designee of the Director whose rank shall be no lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau

field office, certifies that, absent a prohibition of disclosure under this subsection, there may result—

(i) a danger to the national security of the United States;

(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

(iii) interference with diplomatic relations; or

(iv) danger to the life or physical safety of any person.

(2) EXCEPTION.—

(A) IN GENERAL.—A wire or electronic communication service provider, or officer, employee, or agent thereof, that receives a request under subsection (a) may disclose information otherwise subject to any applicable nondisclosure requirement to—

(i) those persons to whom disclosure is necessary in order to comply with the request;

(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

(iii) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(B) PERSONS NECESSARY FOR COMPLIANCE.—Upon a request by the Director of the Federal Bureau of Investigation or the designee of the Director, those persons to whom disclosure will be made under subparagraph (A)(i) or to whom such disclosure was made before the request shall be identified to the Director or the designee.

(C) NONDISCLOSURE REQUIREMENT.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to whom a request is issued under subsection (a) in the same manner as the person to whom the request is issued.

(D) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

(3) RIGHT TO JUDICIAL REVIEW.—

(A) IN GENERAL.—A wire or electronic communications service provider that receives a request under subsection (a) shall have the right to judicial review of any applicable nondisclosure requirement.

(B) NOTIFICATION.—A request under subsection (a) shall state that if the recipient wishes to have a court review a nondisclosure requirement, the recipient shall notify the Government.

(C) INITIATION OF PROCEEDINGS.—If a recipient of a request under subsection (a) makes a notification under subparagraph (B), the Government shall initiate judicial review under the procedures established in section 3511 of this title, unless an appropriate official of the Federal Bureau of Investigation makes a notification under paragraph (4).

(4) TERMINATION.—In the case of any request for which a recipient has submitted a notification under paragraph (3)(B), if the facts supporting a nondisclosure requirement cease to exist, an appropriate official of the Federal Bureau of Investigation shall promptly notify the wire or electronic service provider, or officer, employee, or agent thereof, subject to the nondisclosure requirement that the nondisclosure requirement is no longer in effect.

(e)¿(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.

(f)¿(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.

(g)¿(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.

* * * * * * *

SEC. 3103a. ADDITIONAL GROUNDS FOR ISSUING WARRANT.

(a) IN GENERAL.—In addition to the grounds for issuing a warrant in section 3103 of this title, a warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States.

(b) DELAY.—With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if—

(1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705, except if the adverse results consist only of unduly delaying a trial);

(2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and

(3) the warrant provides for the giving of such notice within a reasonable period not to exceed *7* ¿30 days after the date of its execution, or on a later date certain if the facts of the case justify a longer period of delay.

(c) EXTENSIONS OF DELAY.—Any period of delay authorized by this section may be extended by the court for good cause shown, subject to the condition that extensions should only be granted upon an updated showing of the need for further delay and that each additional delay should be limited to periods of 90 days or less, unless the facts of the case justify a longer period of delay.

(d) REPORTS.—

(1) REPORT BY JUDGE.—Not later than 30 days after the expiration of a warrant authorizing delayed notice (including any extension thereof) entered under this section, or the denial of such warrant (or request for extension), the issuing or denying judge shall report to the Administrative Office of the United States Courts—

(A) the fact that a warrant was applied for;

(B) the fact that the warrant or any extension thereof was granted as applied for, was modified, or was denied;

(C) the period of delay in the giving of notice authorized by the warrant, and the number and duration of any extensions; and

(D) the offense specified in the warrant or application.

(2) REPORT BY ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS.—Beginning with the fiscal year ending September 30, 2007, the Director of the Administrative Office of the United States Courts shall transmit to Congress annually a full and complete report summarizing the data required to be filed with the Administrative Office by paragraph (1), including the number of applications for warrants and extensions of warrants authorizing delayed notice, and the number of such warrants and extensions granted or denied during the preceding fiscal year.

(3) REGULATIONS.—The Director of the Administrative Office of the United States Courts, in consultation with the Attorney General, is authorized to issue binding regulations dealing with the content and form of the reports required to be filed under paragraph (1).

SEC. 3511. JUDICIAL REVIEW OF REQUESTS FOR INFORMATION.

(a) The recipient of a request for records, a report, or other information under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947 may, in the United States district court for the district in which that person or entity does business or resides, petition for an order modifying or setting aside the request. The court may modify or set aside the request if compliance would be unreasonable, oppressive, or otherwise unlawful.

¿(b)(1) The recipient of a request for records, a report, or other information under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947, may petition any court described in sub-

section (a) for an order modifying or setting aside a nondisclosure requirement imposed in connection with such a request.

¿(2) If the petition is filed within one year of the request for records, a report, or other information under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947, the court may modify or set aside such a nondisclosure requirement if it finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person. If, at the time of the petition, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation, or in the case of a request by a department, agency, or instrumentality of the Federal Government other than the Department of Justice, the head or deputy head of such department, agency, or instrumentality, certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations, such certification shall be treated as conclusive unless the court finds that the certification was made in bad faith.

¿(3) If the petition is filed one year or more after the request for records, a report, or other information under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or 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, or in the case of a request by a department, agency, or instrumentality of the Federal Government other than the Federal Bureau of Investigation, the head or deputy head of such department, agency, or instrumentality, within ninety days of the filing of the petition, shall either terminate the nondisclosure requirement or re-certify that disclosure may result in 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. In the event of re-certification, the court may modify or set aside such a nondisclosure requirement if it finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person. If the recertification that disclosure may endanger the national security of the United States or interfere with diplomatic relations is made by the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation, such certification shall be treated as conclusive unless the court finds that the recertification was made in bad faith. If the court denies a petition for an order modifying or setting aside a nondisclosure requirement under this

paragraph, the recipient shall be precluded for a period of one year from filing another petition to modify or set aside such nondisclosure requirement.

(b) NONDISCLOSURE.—

(1) IN GENERAL.—

(A) NOTICE.—If a recipient of a request or order for a report, records, or other information under section 2709 of this title, section 626 or 627 of the Fair Credit Reporting Act (15 U.S.C. 1681u and 1681v), section 1114 of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414), or section 802 of the National Security Act of 1947 (50 U.S.C. 436), wishes to have a court review a nondisclosure requirement imposed in connection with the request or order, the recipient shall notify the Government.

(B) APPLICATION.—Not later than 30 days after the date of receipt of a notification under subparagraph (A), the Government shall apply for an order prohibiting the disclosure of the existence or contents of the relevant request or order. An application under this subparagraph may be filed in the district court of the United States for the judicial district in which the recipient of the order is doing business or in the district court of the United States for any district within which the authorized investigation that is the basis for the request or order is being conducted. The applicable nondisclosure requirement shall remain in effect during the pendency of proceedings relating to the requirement.

(C) CONSIDERATION.—A district court of the United States that receives an application under subparagraph (B) should rule expeditiously, and shall, subject to paragraph (3), issue a nondisclosure order that includes conditions appropriate to the circumstances.

(2) APPLICATION CONTENTS.—An application for a nondisclosure order or extension thereof under this subsection shall include a certification from the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation, or in the case of a request by a department, agency, or instrumentality of the Federal Government other than the Department of Justice, the head or deputy head of the department, agency, or instrumentality, containing a statement of specific facts indicating that, absent a prohibition of disclosure under this subsection, there may result—

(A) a danger to the national security of the United States;

(B) interference with a criminal, counterterrorism, or counterintelligence investigation;

(C) interference with diplomatic relations; or

(D) danger to the life or physical safety of any person.

(3) STANDARD.—A district court of the United States shall issue a nondisclosure requirement order or extension thereof under this subsection if the court determines, giving substantial weight to the certification under paragraph (2) that there is reason to believe that disclosure of the information subject to the nondisclosure requirement during the applicable time period will result in—

(A) a danger to the national security of the United States;

(B) interference with a criminal, counterterrorism, or counterintelligence investigation;

(C) interference with diplomatic relations; or

(D) danger to the life or physical safety of any person.

(c) In the case of a failure to comply with a request for records, a report, or other information made to any person or entity under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947, the Attorney General may invoke the aid of any district court of the United States within the jurisdiction in which the investigation is carried on or the person or entity resides, carries on business, or may be found, to compel compliance with the request. The court may issue an order requiring the person or entity to comply with the request. Any failure to obey the order of the court may be punished by the court as contempt thereof. Any process under this section may be served in any judicial district in which the person or entity may be found.

(d) In all proceedings under this section, subject to any right to an open hearing in a contempt proceeding, the court must close any hearing to the extent necessary to prevent an unauthorized disclosure of a request for records, a report, or other information made to any person or entity under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947. Petitions, filings, records, orders, and subpoenas must also be kept under seal to the extent and as long as necessary to prevent the unauthorized disclosure of a request for records, a report, or other information made to any person or entity under section 2709(b) of this title, section 626(a) or (b) or 627(a) of the Fair Credit Reporting Act, section 1114(a)(5)(A) of the Right to Financial Privacy Act, or section 802(a) of the National Security Act of 1947.

(e) In all proceedings under this section, the court shall, upon request of the government, review ex parte and in camera any government submission or portions thereof, which may include classified information.

* * * * * * *

TITLE 42—THE PUBLIC HEALTH AND WELFARE

CHAPTER 23—Development and Control of Atomic Energy Division a. Atomic Energy

Subchapter XVII. Enforcement of Chapter

SEC. 2272. VIOLATION OF SPECIFIC SECTIONS.

(a) Whoever willfully violates, attempts to violate, or conspires to violate, any provision of sections 2077 or 2131 of this title, or whoever unlawfully interferes, attempts to interfere, or conspires to interfere with any recapture or entry under section 2138 of this title, shall, upon conviction thereof, be punished by a fine of not more than $10,000 or by imprisonment for not more than ten

years, or both, except that whoever commits such an offense with intent to injure the United States or with intent to secure an advantage to any foreign nation shall, upon conviction thereof, be punished by imprisonment for life, or by imprisonment for any term of years or a fine of not more than $20,000 *or* both.

(b) Any person who violates, or attempts or conspires to violate, section 2122 of this title shall be fined not more than $2,000,000 and sentenced to a term of imprisonment not less than 25 years or to imprisonment for life. Any person who, in the course of a violation of section 2122 of this title, uses, attempts or conspires to use, or possesses and threatens to use, any atomic weapon shall be fined not more than $2,000,000 and imprisoned for not less than 30 years or imprisoned for life. If the death of another results from a person's violation of section 2122 of this title, the person shall be fined not more than $2,000,000 and punished by *death or* imprisonment for life.

* * * * * * *

TITLE 50—WAR AND NATIONAL DEFENSE

* * * * * * *

CHAPTER 15—NATIONAL SECURITY

Subchapter VI—Access to Classified Information

SEC. 436. REQUESTS BY AUTHORIZED INVESTIGATIVE AGENCIES.

(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.

(4) A department or agency head, deputy department or agency head, or senior official described in paragraph (3)(A) may make a certification under paragraph (3)(A) only upon a written statement, which shall be retained by the authorized investigative agency, of specific facts showing that there are reasonable grounds to believe that the information sought is relevant to the authorized inquiry or investigation described in paragraph (3)(A)(ii).

¿(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.

(b) PROHIBITION OF CERTAIN DISCLOSURE.—

(1) PROHIBITION.—

(A) IN GENERAL.—If a certification is issued under subparagraph (B) and notice of the right to judicial review under paragraph (4) is provided, no governmental or private entity, or officer, employee, or agent thereof, that receives a request under subsection (a), shall disclose to any person the particular information specified in the certification during the time period to which the certification applies, which may be not longer than 1 year.

(B) CERTIFICATION.—The requirements of subparagraph (A) shall apply if the head of an authorized investigative agency described in subsection (a), or a designee, certifies that, absent a prohibition of disclosure under this subsection, there may result—

(i) a danger to the national security of the United States;

(ii) interference with a criminal, counterterrorism, or counterintelligence investigation;

(iii) interference with diplomatic relations; or

(iv) danger to the life or physical safety of any person.

(2) EXCEPTION.—

(A) IN GENERAL.—A governmental or private entity, or officer, employee, or agent thereof, that receives a request under subsection (a) may disclose information otherwise subject to any applicable nondisclosure requirement to—

(i) those persons to whom disclosure is necessary in order to comply with the request;

(ii) an attorney in order to obtain legal advice or assistance regarding the request; or

(iii) other persons as permitted by the head of the authorized investigative agency described in subsection (a).

(B) NONDISCLOSURE REQUIREMENT.—A person to whom disclosure is made under subparagraph (A) shall be subject to the nondisclosure requirements applicable to a person to

whom a request is issued under subsection (a) in the same manner as the person to whom the request is issued.

(C) NOTICE.—Any recipient that discloses to a person described in subparagraph (A) information otherwise subject to a nondisclosure requirement shall inform the person of the applicable nondisclosure requirement.

(3) EXTENSION.—The head of an authorized investigative agency described in subsection (a), or a designee, may extend a nondisclosure requirement for additional periods of not longer than 1 year if, at the time of each extension, a new certification is made under paragraph (1)(B) and notice is provided to the recipient of the applicable request that the nondisclosure requirement has been extended and the recipient has the right to judicial review of the nondisclosure requirement.

(4) RIGHT TO JUDICIAL REVIEW.—

(A) IN GENERAL.—A governmental or private entity that receives a request under subsection (a) shall have the right to judicial review of any applicable nondisclosure requirement and any extension thereof.

(B) TIMING.—

(i) IN GENERAL.—A request under subsection (a) shall state that if the recipient wishes to have a court review a nondisclosure requirement, the recipient shall notify the Government not later than 21 days after the date of receipt of the request.

(ii) EXTENSION.—A notice that the applicable nondisclosure requirement has been extended under paragraph (3) shall state that if the recipient wishes to have a court review the nondisclosure requirement, the recipient shall notify the Government not later than 21 days after the date of receipt of the notice.

(C) INITIATION OF PROCEEDINGS.—If a recipient of a request under subsection (a) makes a notification under subparagraph (B), the Government shall initiate judicial review under the procedures established in section 3511 of title 18, United States Code.

(5) TERMINATION.—If the facts supporting a nondisclosure requirement cease to exist prior to the applicable time period of the nondisclosure requirement, an appropriate official of the authorized investigative agency described in subsection (a) shall promptly notify the governmental or private entity, or officer, employee, or agent thereof, subject to the nondisclosure requirement that the nondisclosure requirement is no longer in effect.

(c) RECORDS OR INFORMATION; INSPECTION OR COPYING.—

(1) Notwithstanding any other provision of law (other than section 6103 of Title 26), an entity receiving a request for records or information under subsection (a) of this section shall, if the request satisfies the requirements of this section, make available such records or information within 30 days for inspection or copying, as may be appropriate, by the agency requesting such records or information.

(2) Any entity (including any officer, employee, or agent thereof) that discloses records or information for inspection or copying pursuant to this section in good faith reliance upon the

certifications made by an agency pursuant to this section shall not be liable for any such disclosure to any person under this subchapter, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

(d) REIMBURSEMENT OF COSTS.—Any agency requesting records or information under this section may, subject to the availability of appropriations, reimburse a private entity for any cost reasonably incurred by such entity in responding to such request, including the cost of identifying, reproducing, or transporting records or other data.

(e) DISSEMINATION OF RECORDS OR INFORMATION RECEIVED.—An agency receiving records or information pursuant to a request under this section may disseminate the records or information obtained pursuant to such request outside the agency only—

(1) to the agency employing the employee who is the subject of the records or information;

(2) to the Department of Justice for law enforcement or counterintelligence purposes; or

(3) with respect to dissemination to an agency of the United States, if such information is clearly relevant to the authorized responsibilities of such agency.

(f) CONSTRUCTION OF SECTION.—Nothing in this section may be construed to affect the authority of an investigative agency to obtain information pursuant to the Right to Financial Privacy Act (12 U.S.C. 3401 et seq.) or the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

* * * * * * *

CHAPTER 36—FOREIGN INTELLIGENCE SURVEILLANCE

Subchapter I—Electronic Surveillance

SEC. 1805. ISSUANCE OF AN ORDER.

(a) NECESSARY FINDINGS.—Upon an application made pursuant to section 1804 of this title, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that—

(1) the application has been made by a Federal officer and approved by the Attorney General;

(2) on the basis of the facts submitted by the applicant there is probable cause to believe that—

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(3) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title; and

(4) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

(b) DETERMINATION OF PROBABLE CAUSE.—In determining whether or not probable cause exists for purposes of an order under subsection (a)(2) of this section, a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.

(c) SPECIFICATIONS AND DIRECTIONS OF ORDERS.—

(1) SPECIFICATIONS.—An order approving an electronic surveillance under this section shall specify—

(A) the identity, if known, or a description *with particularity* of the specific target of the electronic surveillance identified or described in the application pursuant to section 1804(a)(3) of this title;

(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known;

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance; and

(E) the period of time during which the electronic surveillance is approved.

Subchapter III—Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes

SEC. 1841. DEFINITION.

As used in this subchapter:

(1) The terms "foreign power", "agent of a foreign power", "international terrorism", "foreign intelligence information", "Attorney General", "United States person", "United States", "person", and "State" shall have the same meanings as in section 1801 of this title.

(2) The terms "pen register" and "trap and trace device" have the meanings given such terms in section 3127 of Title 18.

(3) The term "aggrieved person" means any person—

(A) whose telephone line was subject to the installation or use of a pen register or trap and trace device authorized by this subchapter; or

(B) whose communication instrument or device was subject to the use of a pen register or trap and trace device authorized by this subchapter to capture incoming electronic or other communications impulses.

(4) THE TERM "MINIMIZATION PROCEDURES" MEANS.—

(A) specific procedures, that are reasonably designed in light of the purpose and technique of an order for the installation and use of a pen register or trap and trace de-

vice, to minimize the retention, and prohibit the dissemination, of nonpublicly available information known to concern unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(B) procedures that require that nonpublicly available information, which is not foreign intelligence information 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; and

(C) notwithstanding subparagraphs (A) and (B), 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.

SEC. 1842. PEN REGISTERS AND TRAP AND TRACE DEVICES FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.

(a) APPLICATION FOR AUTHORIZATION OR APPROVAL.—

(1) Notwithstanding any other provision of law, the Attorney General or a designated attorney for the Government may make an application for an order or an extension of an order authorizing or approving the installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution which is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.

(2) The authority under paragraph (1) is in addition to the authority under subchapter I of this chapter to conduct the electronic surveillance referred to in that paragraph.

(b) FORM OF APPLICATION; RECIPIENT.—Each application under this section shall be in writing under oath or affirmation to—

(1) a judge of the court established by section 1803(a) of this title; or

(2) a United States Magistrate Judge under chapter 43 of Title 28, who is publicly designated by the Chief Justice of the United States to have the power to hear applications for and grant orders approving the installation and use of a pen register or trap and trace device on behalf of a judge of that court.

(c) EXECUTIVE APPROVAL; CONTENTS OF APPLICATION.—Each application under this section shall require the approval of the Attorney General, or a designated attorney for the Government, and shall include—

(1) the identity of the Federal officer seeking to use the pen register or trap and trace device covered by the application; ¿and

(2) ¿a certification by the applicant *a statement of the facts and circumstances relied upon by the applicant to justify the belief of the applicant* that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution¿. *; and*

(3) a statement of whether minimization procedures are being proposed and, if so, a statement of the proposed minimization procedures.

(d) EX PARTE JUDICIAL ORDER OF APPROVAL.—

(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the installation and use of a pen register or trap and trace device if ¿the judge finds that the application satisfies the requirements of this section. *the judge finds—*

(A) that the application satisfies the requirements of this section; and

(B) that, if there are exceptional circumstances justifying the use of minimization procedures in a particular case, the proposed minimization procedures meet the definition of minimization procedures under this title.

(2) An order issued under this section—

(A) shall specify—

(i) the identity, if known, of the person who is the subject of the investigation;

(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied; and

(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order;

(B) shall direct that—

(i) upon request of the applicant, the provider of a wire or electronic communication service, landlord, custodian, or other person shall furnish any information, facilities, or technical assistance necessary to accomplish the installation and operation of the pen register or trap and trace device in such a manner as will protect its secrecy and produce a minimum amount of interference with the services that such provider, landlord, custodian, or other person is providing the person concerned;

(ii) such provider, landlord, custodian, or other person—

(I) shall not disclose the existence of the investigation or of the pen register or trap and trace

device to any person unless or until ordered by the court; and

(II) shall maintain, under security procedures approved by the Attorney General and the Director of National Intelligence pursuant to section 1805(b)(2)(C) of this title, any records concerning the pen register or trap and trace device or the aid furnished; ¿and

(iii) the applicant shall compensate such provider, landlord, custodian, or other person for reasonable expenses incurred by such provider, landlord, custodian, or other person in providing such information, facilities, or technical assistance; and

(iv) if applicable, the minimization procedures be followed; and

(C) shall direct that, upon the request of the applicant, the provider of a wire or electronic communication service shall disclose to the Federal officer using the pen register or trap and trace device covered by the order—

(i) in the case of the customer or subscriber using the service covered by the order (for the period specified by the order)—

(I) the name of the customer or subscriber;

(II) the address of the customer or subscriber;

(III) the telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber, including any temporarily assigned network address or associated routing or transmission information;

(IV) the length of the provision of service by such provider to the customer or subscriber and the types of services utilized by the customer or subscriber;

(V) in the case of a provider of local or long distance telephone service, any local or long distance telephone records of the customer or subscriber;

(VI) if applicable, any records reflecting period of usage (or sessions) by the customer or subscriber; and

(VII) any mechanisms and sources of payment for such service, including the number of any credit card or bank account utilized for payment for such service; and

(ii) if available, with respect to any customer or subscriber of incoming or outgoing communications to or from the service covered by the order—

(I) the name of such customer or subscriber;

(II) the address of such customer or subscriber;

(III) the telephone or instrument number, or other subscriber number or identifier, of such customer or subscriber, including any temporarily assigned network address or associated routing or transmission information; and

(IV) the length of the provision of service by such provider to such customer or subscriber and the types of services utilized by such customer or subscriber.

(e) TIME LIMITATION.—

(1) Except as provided in paragraph (2), an order issued under this section shall authorize the installation and use of a pen register or trap and trace device for a period not to exceed 90 days. Extensions of such an order may be granted, but only upon an application for an order under this section and upon the judicial finding required by subsection (d) of this section. The period of extension shall be for a period not to exceed 90 days.

(2) In the case of an application under subsection (c) of this section where the applicant has certified that the information likely to be obtained is foreign intelligence information not concerning a United States person, an order, or an extension of an order, under this section may be for a period not to exceed one year.

(f) CAUSE OF ACTION BARRED.—No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance under subsection (d) of this section in accordance with the terms of an order issued under this section.

(g) FURNISHING OF RESULTS.—Unless otherwise ordered by the judge, the results of a pen register or trap and trace device shall be furnished at reasonable intervals during regular business hours for the duration of the order to the authorized Government official or officials.

(h) At or before the end of the period of time for which the installation and use of a pen register or trap and trace device is approved under an order or an extension under this section, the judge may assess compliance with any applicable minimization procedures by reviewing the circumstances under which information concerning United States persons was retained or disseminated.

SEC. 1843. AUTHORIZATION DURING EMERGENCIES.

(a) REQUIREMENTS FOR AUTHORIZATION.—Notwithstanding any other provision of this subchapter, when the Attorney General makes a determination described in subsection (b) of this section, the Attorney General may authorize the installation and use of a pen register or trap and trace device on an emergency basis to gather foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution if—

(1) a judge referred to in section 1842(b) of this title is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to install and use the pen register or trap and trace device, as the case may be, on an emergency basis; and

(2) an application in accordance with section 1842 of this title is made to such judge as soon as practicable, but not more than 7 days, after the Attorney General authorizes the installation and use of the pen register or trap and trace device, as the case may be, under this section.

(b) DETERMINATION OF EMERGENCY AND FACTUAL BASIS.—A determination under this subsection is a reasonable determination by the Attorney General that—

(1) an emergency requires the installation and use of a pen register or trap and trace device to obtain foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution before an order authorizing the installation and use of the pen register or trap and trace device, as the case may be, can with due diligence be obtained under section 1842 of this title; and

(2) the factual basis for issuance of an order under such section 1842 of this title to approve the installation and use of the pen register or trap and trace device, as the case may be, exists.

(c) If the Attorney General authorizes the emergency installation and use of a pen register or trap and trace device under this section, the Attorney General shall require that minimization procedures be followed, if appropriate.

(*d*)¿(c) EFFECT OF ABSENCE OF ORDER.—

(1) In the absence of an order applied for under subsection (a)(2) of this section approving the installation and use of a pen register or trap and trace device authorized under this section, the installation and use of the pen register or trap and trace device, as the case may be, shall terminate at the earlier of—

(A) when the information sought is obtained;

(B) when the application for the order is denied under section 1842 of this title; or

(C) 7 days after the time of the authorization by the Attorney General.

(2) In the event that an application for an order applied for under subsection (a)(2) of this section is denied, or in any other case where the installation and use of a pen register or trap and trace device under this section is terminated and no order under section 1842 of this title is issued approving the installation and use of the pen register or trap and trace device, as the case may be, no information obtained or evidence derived from the use of the pen register or trap and trace device, as the case may be, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from the use of the pen register or trap and trace device, as the case may be, shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent

of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

SEC. 1845. USE OF INFORMATION.

(a) IN GENERAL.—

(1) Information acquired from the use of a pen register or trap and trace device installed pursuant to this subchapter 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 ¿provisions of this section *minimization procedures required under this title.*

(2) No information acquired from a pen register or trap and trace device installed and used pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.

* * * * * * *

CHAPTER 36—FOREIGN INTELLIGENCE SURVEILLANCE

Subchapter IV—Access to Certain Business Records *and Other Tangible Things* for Foreign Intelligence Purposes

SEC. 501. ACCESS TO CERTAIN BUSINESS RECORDS *AND OTHER TANGIBLE THINGS* FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.

(a)(1) Subject to paragraph (3), the Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

(2) An investigation conducted under this section shall—

(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(3) In the case of an application for an order requiring the production of 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, the Director of the Federal Bureau of Investigation may delegate the authority to make such application to either the Deputy Director of the Federal Bureau of Investigation or the Executive Assistant Director for National Security (or any successor position). The Deputy Director or the Executive Assistant Director may not further delegate such authority.

(b) Each application under this section—

(1) shall be made to—

(A) a judge of the court established by section 1803(a) of this title; or

(B) a United States Magistrate Judge under chapter 43 of Title 28, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

(2) shall include—

(A) ¿a statement of facts showing *a statement of the facts and circumstances relied upon by the applicant to justify the belief of the applicant* that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) of this section to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or *clandestine intelligence activities;* ¿clandestine intelligence activities, such things being presumptively relevant to an authorized investigation if the applicant shows in the statement of the facts that they pertain to—

¿(i) a foreign power or an agent of a foreign power;

¿(ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or

¿(iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation; and

¿(B) an enumeration of the minimization procedures adopted by the Attorney General under subsection (g) of this section that are applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be made available to the Federal Bureau of Investigation based on the order requested in such application.

(B) if the records sought contain bookseller records, or are from a library and contain personally identifiable information about a patron of the library, a statement of facts showing that there are reasonable grounds to believe that the records sought—

(i) are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities; and

(ii)(I) pertain to a foreign power or an agent of a foreign power;

(II) are relevant to the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or

(III) pertain to an individual in contact with, or known to, a suspected agent of a foreign power; and

(C) a statement of proposed minimization procedures.

(c)(1) Upon an application made pursuant to this section, if the judge finds that the application meets the requirements of subsections (a) and (b) *and that the proposed minimization procedures meet the definition of minimization procedures under subsection (g)* of this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of tangible things*, and directing that the minimization procedures be followed.* ¿Such order shall direct that minimization procedures adopted pursuant to subsection (g) of this section be followed.

(2) An order under this subsection—

(A) shall describe the tangible things that are ordered to be produced with sufficient particularity to permit them to be fairly identified;

(B) shall include the date on which the tangible things must be provided, which shall allow a reasonable period of time within which the tangible things can be assembled and made available;

(C) shall provide clear and conspicuous notice of the principles and procedures described in subsection (d) of this section;

(D) may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things; ¿and

(E) shall not disclose that such order is issued for purposes of an investigation described in subsection (a) of this section¿. *; and*

(F) shall direct that the minimization procedures be followed.

(d)(1) No person shall disclose to any other person that the Federal bureau of investigation has sought or obtained tangible things pursuant to an order under this section, other than to—

(A) those persons to whom disclosure is necessary to comply with such order;

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

(C) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(2)(A) A person to whom disclosure is made pursuant to paragraph (1) shall be subject to the nondisclosure requirements applicable to a person to whom an order is directed under this section in the same manner as such person.

(B) Any person who discloses to a person described in subparagraph (A), (B), or (C) of paragraph (1) that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section shall notify such person of the nondisclosure requirements of this subsection.

(C) 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 subparagraph (A) or (C) of

paragraph (1) 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.

(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

(f)(1) In this subsection—

(A) the term ''production order'' means an order to produce any tangible thing under this section; and

(B) the term ''nondisclosure order'' means an order imposed under subsection (d) of this section.

(2)(A)(i) A person receiving ¿a production order *a production order or nondisclosure order* may challenge the legality of that order by filing a petition with the pool established by section 1803(e)(1) of this title. ¿Not less than 1 year after the date of the issuance of the production order, the recipient of a production order may challenge the nondisclosure order imposed in connection with such production order by filing a petition to modify or set aside such nondisclosure order, consistent with the requirements of subparagraph (C), with the pool established by section 1803(e)(1) of this title.

(ii) The presiding judge shall immediately assign a petition under clause (i) to 1 of the judges serving in the pool established by section 1803(e)(1) of this title. Not later than 72 hours after the assignment of such petition, the assigned judge shall conduct an initial review of the petition. If the assigned judge determines that the petition is frivolous, the assigned judge shall immediately deny the petition and affirm the ¿production order or nondisclosure order. If the assigned judge determines the petition is not frivolous, the assigned judge shall promptly consider the petition in accordance with the procedures established under section 1803(e)(2) of this title.

(iii) The assigned judge shall promptly provide a written statement for the record of the reasons for any determination under this subsection. Upon the request of the Government, any order setting aside a nondisclosure order shall be stayed pending review pursuant to paragraph (3).

(B) A judge considering a petition to modify or set aside a production order may grant such petition only if the judge finds that such order does not meet the requirements of this section or is otherwise unlawful. If the judge does not modify or set aside the production order, the judge shall immediately affirm such order, and order the recipient to comply therewith.

(C)(i) A judge considering a petition to modify or set aside a nondisclosure order may grant such petition only if the judge finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.

¿(ii) If, upon filing of such a petition, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Direc-

tor of the Federal Bureau of Investigation certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations, such certification shall be treated as conclusive, unless the judge finds that the certification was made in bad faith.

(ii)¿(iii) If the judge denies a petition to modify or set aside a nondisclosure order, the recipient of such order shall be precluded for a period of 1 year from filing another such petition with respect to such nondisclosure order.

(D) Any production or nondisclosure order not explicitly modified or set aside consistent with this subsection shall remain in full effect.

(3) A petition for review of a decision under paragraph (2) to affirm, modify, or set aside an order by the Government or any person receiving such order shall be made to the court of review established under section 1803(b) of this title, which shall have jurisdiction to consider such petitions. The court of review shall provide for the record a written statement of the reasons for its decision and, on petition by the Government or any person receiving such order for writ of certiorari, the record shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(4) Judicial proceedings under this subsection shall be concluded as expeditiously as possible. The record of proceedings, including petitions 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.

(5) All petitions under this subsection shall be filed under seal. In any proceedings under this subsection, the court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions thereof, which may include classified information.

(g) MINIMIZATION PROCEDURES.—

(1) IN GENERAL.—¿Not later than 180 days after March 9, 2006, the Attorney General shall adopt specific minimization procedures governing the retention and dissemination by the Federal Bureau of Investigation of any tangible things, or information therein, received by the Federal Bureau of Investigation in response to an order under this subchapter. *At or before the end of the period of time for the production of tangible things under an order approved under this section or at any time after the production of tangible things under an order approved under this section, a judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was retained or disseminated.*

(2) DEFINED.—In this section, the term "minimization procedures" means—

(A) specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the 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;

(B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 1801(e)(1) of this title, 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; and

(C) notwithstanding subparagraphs (A) and (B), 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.

(h) USE OF INFORMATION.—Information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this subchapter 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 (g) of this section. No otherwise privileged information acquired from tangible things received by the Federal Bureau of Investigation in accordance with the provisions of this subchapter shall lose its privileged character. No information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.

(i) DEFINITIONS.—In this section—

(1) the term "bookseller records" means transactional records reflecting the purchase (including subscription purchase) or rental of books, journals, or magazines, whether in digital form or in print, of an individuals or entity engaged in the sale or rental of books, journals, or magazines;

(2) the term "library" has the meaning given that term in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1));

(3) the term "patron" means a purchaser, renter, borrower, user, or subscriber of goods or services from a library; and

(4) the term "personally identifiable information" includes information that identifies a person as having used, requested, or obtained specific reading materials or services from a library.

SEC. 503. DEFINITIONS.

In this title, the terms "Attorney General", "foreign intelligence information", "international terrorism", "person", "United States", and "United States person" have the meanings given such terms in section 101.

* * * * * * *

Subchapter V—Reporting Requirement

SEC. 601. SEMIANNUAL REPORT OF THE ATTORNEY GENERAL.

(a) REPORT.—On a semiannual basis, the Attorney General shall submit to the Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of

the Senate, and the Committees on the Judiciary of the House of Representatives and the Senate, in a manner consistent with the protection of the national security, a report setting forth with respect to the preceding 6-month period—

(1) the aggregate number of persons targeted for orders issued under this chapter, including a breakdown of those targeted for—

(A) electronic surveillance under section 1805 of this title;

(B) physical searches under section 1824 of this title;

(C) pen registers under section 1842 of this title;

(D) access to records under section 1861 of this title;

(E) acquisitions under section 1881b of this title; and

(F) acquisitions under section 1881c of this title;

(2) the number of individuals covered by an order issued pursuant to section 1801(b)(1)(C) of this title;

(3) the number of times that the Attorney General has authorized that information obtained under this chapter may be used in a criminal proceeding or any information derived therefrom may be used in a criminal proceeding;

(4) a summary of significant legal interpretations of this chapter involving matters before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, including interpretations presented in applications or pleadings filed with the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review by the Department of Justice; and

(5) copies of all decisions, orders, or opinions of the Foreign Intelligence Surveillance Court or Foreign Intelligence Surveillance Court of Review that include significant construction or interpretation of the provisions of this chapter.

(b) FREQUENCY.—The first report under this section shall be submitted not later than 6 months after December 17, 2004. Subsequent reports under this section shall be submitted semi-annually thereafter.

(c) SUBMISSIONS TO CONGRESS.—The Attorney General shall submit to the committees of Congress referred to in subsection (a)—

(1) a copy of any decision, order, or opinion issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review that includes significant construction or interpretation of any provision of this chapter, and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion, not later than 45 days after such decision, order, or opinion is issued; and

(2) a copy of each such decision, order, or opinion, and any pleadings, applications, or memoranda of law associated with such decision, order, or opinion, that was issued during the 5-year period ending on July 10, 2008 and not previously submitted in a report under subsection (a).

(d) PROTECTION OF NATIONAL SECURITY.—The Attorney General, in consultation with the Director of National Intelligence, may authorize redactions of materials described in subsection (c) that are provided to the committees of Congress referred to in subsection (a), if such redactions are necessary to protect the national security

of the United States and are limited to sensitive sources and methods information or the identities of targets.

(e) DEFINITIONS.—In this section:

(1) FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The term "Foreign Intelligence Surveillance Court" means the court established under section 1803(a) of this title.

(2) FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW.—The term "Foreign Intelligence Surveillance Court of Review" means the court established under section 1803(b) of this title.

SEC. 602. ANNUAL UNCLASSIFIED REPORT.

Not later than June 30, 2012, and every year thereafter, the Attorney General, in consultation with the Director of National Intelligence, and with due regard for the protection of classified information from unauthorized disclosure, shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives an unclassified report summarizing how the authorities under this Act are used, including the impact of the use of the authorities under this Act on the privacy of United States persons (as defined in section 101).

* * * * * * *

USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT OF 2005

P.L. 109–177 (H.R. 3199)

SEC. 102. USA PATRIOT ACT SUNSET PROVISIONS.

(a) IN GENERAL.—Section 224 of the USA PATRIOT Act is repealed.

(b) SECTIONS 206 AND 215 SUNSET.—

(1) IN GENERAL.—Effective ¿May 27, 2011 *December 31, 2013*, the Foreign Intelligence Surveillance Act of 1978 is amended so that sections 501, 502, and 105(c)(2) read as they read on October 25, 2001.

(2) EXCEPTION.—With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in paragraph (1) cease to have effect, or with respect to any particular offense or potential offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect.

* * * * * * *

SEC. 106A. AUDIT ON ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE PURPOSES.

(a) AUDIT.—The Inspector General of the Department of Justice shall perform a comprehensive audit of the effectiveness and use, including any improper or illegal use, of the investigative authority provided to the Federal Bureau of Investigation under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.).

(b) REQUIREMENTS.—The audit required under subsection (a) shall include—

(1) an examination of each instance in which the Attorney General, any other officer, employee, or agent of the Department of Justice, the Director of the Federal Bureau of Investigation, or a designee of the Director, submitted an application to the Foreign Intelligence Surveillance Court (as such term is defined in section 301(3) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1821(3))) for an order under section 501 of such Act during the calendar years of 2002 through *2011* ¿2006 , including—

(A) whether the Federal Bureau of Investigation requested that the Department of Justice submit an application and the request was not submitted to the court (including an examination of the basis for not submitting the application);

(B) whether the court granted, modified, or denied the application (including an examination of the basis for any modification or denial);

¿(2) the justification for the failure of the Attorney General to issue implementing procedures governing requests for the production of tangible things under such section in a timely fashion, including whether such delay harmed national security;

¿(3) whether bureaucratic or procedural impediments to the use of such requests for production prevent the Federal Bureau of Investigation from taking full advantage of the authorities provided under section 501 of such Act;

(2)¿(4) any noteworthy facts or circumstances relating to orders under such section, including any improper or illegal use of the authority provided under such section; and

(3)¿(5) an examination of the effectiveness of such section as an investigative tool, including—

(A) the categories of records obtained and the importance of the information acquired to the intelligence activities of the Federal Bureau of Investigation or any other Department or agency of the Federal Government;

(B) the manner in which such information is collected, retained, analyzed, and disseminated by the Federal Bureau of Investigation, including any direct access to such information (such as access to "raw data") provided to any other Department, agency, or instrumentality of Federal, State, local, or tribal governments or any private sector entity;

¿(C) with respect to calendar year 2006, an examination of the minimization procedures adopted by the Attorney General under section 501(g) of such Act and whether such minimization procedures protect the constitutional rights of United States persons;

(C) with respect to calendar years 2007 through 2011, an examination of the minimization procedures used in relation to orders under section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861) and whether the

minimization procedures protect the constitutional rights of United States persons;

(D) whether, and how often, the Federal Bureau of Investigation utilized information acquired pursuant to an order under section 501 of such Act to produce an analytical intelligence product for distribution within the Federal Bureau of Investigation, to the intelligence community ¿(as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4))) , or to other Federal, State, local, or tribal government Departments, agencies, or instrumentalities; and

(E) whether, and how often, the Federal Bureau of Investigation provided such information to law enforcement authorities for use in criminal proceedings.

(c) SUBMISSION DATES.—

(1) PRIOR YEARS.—Not later than one year after the date of the enactment of this Act, or upon completion of the audit under this section for calendar years 2002, 2003, and 2004, whichever is earlier, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary and the Select Committee on Intelligence of the Senate a report containing the results of the audit conducted under this section for calendar years 2002, 2003, and 2004.

(2) CALENDAR YEARS 2005 AND 2006.—Not later than December 31, 2007, or upon completion of the audit under this section for calendar years 2005 and 2006, whichever is earlier, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary and the Select Committee on Intelligence of the Senate a report containing the results of the audit conducted under this section for calendar years 2005 and 2006.

(3) CALENDAR YEARS 2007, 2008, AND 2009.—Not later than March 31, 2012, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary and the Select Committee on Intelligence of the Senate a report containing the results of the audit conducted under subsection (a) for calendar years 2007, 2008, and 2009.

(4) CALENDAR YEARS 2010 AND 2011.—Not later than March 31, 2013, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary and the Select Committee on Intelligence of the Senate a report containing the results of the audit conducted under subsection (a) for calendar years 2010 and 2011.

(d) INTELLIGENCE ASSESSMENT.—

(1) IN GENERAL.—For the period beginning on January 1, 2007 and ending on December 31, 2011, the Inspector General

of each element of the intelligence community outside of the Department of Justice that used information acquired under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) in the intelligence activities of the element of the intelligence community shall—

(A) assess the importance of the information to the intelligence activities of the element of the intelligence community;

(B) examine the manner in which that information was collected, retained, analyzed, and disseminated by the element of the intelligence community;

(C) describe any noteworthy facts or circumstances relating to orders under title V of the Foreign Intelligence Surveillance Act of 1978 as the orders relate to the element of the intelligence community; and

(D) examine any minimization procedures used by the element of the intelligence community under title V of the Foreign Intelligence Surveillance Act of 1978 and whether the minimization procedures protect the constitutional rights of United States persons.

(2) SUBMISSION DATES FOR ASSESSMENT.—

(A) CALENDAR YEARS 2007 THROUGH 2009.—Not later than March 31, 2012, the Inspector General of each element of the intelligence community that conducts an assessment under this subsection shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representative a report containing the results of the assessment for calendar years 2007 through 2009.

(B) CALENDAR YEARS 2010 AND 2011.—Not later than March 31, 2013, the Inspector General of each element of the intelligence community that conducts an assessment under this subsection shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives a report containing the results of the assessment for calendar years 2010 and 2011.

(e)¿(d) PRIOR NOTICE TO ATTORNEY GENERAL AND DIRECTOR OF NATIONAL INTELLIGENCE; COMMENTS.—

(1) NOTICE.—Not less than 30 days before the submission of ¿a report under subsection (c)(1) or (c)(2) *any report under subsection (c) or (d),* the Inspector General of the Department of Justice *and any Inspector General of an element of the intelligence community that submits a report under this section* shall provide such report to the Attorney General and the Director of National Intelligence.

(2) COMMENTS.—The Attorney General or the Director of National Intelligence may provide comments to be included in ¿the reports submitted under subsections (c)(1) and (c)(2) *any report submitted under subsection (c) or (d)* as the Attorney General or the Director of National Intelligence may consider necessary.

(f)¿(e) UNCLASSIFIED FORM.—¿The reports submitted under subsections (c)(1) and (c)(2) *Each report submitted under subsection (c)* and any comments included under ¿subsection (d)(2) *subsection (e)(2)* shall be in unclassified form, but may include a classified annex.

(g) DEFINITIONS.—In this section—

(1) the term "intelligence community" has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 401a); and

(2) the term "United States person" has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

* * * * * * *

SECTION 118. REPORTS ON NATIONAL SECURITY LETTERS.

* * * * * * *

¿(c) REPORT ON REQUESTS FOR NATIONAL SECURITY LETTERS.—

¿(1) IN GENERAL.—In April of each year, the Attorney General shall submit to Congress an aggregate report setting forth with respect to the preceding year the total number of requests made by the Department of Justice for information concerning different United States persons under—

¿(A) section 2709 of title 18, United States Code (to access certain communication service provider records), excluding the number of requests for subscriber information;

¿(B) section 1114 of the Right to Financial Privacy Act (12 U.S.C. 3414) (to obtain financial institution customer records);

¿(C) section 802 of the National Security Act of 1947 (50 U.S.C. 436) (to obtain financial information, records, and consumer reports);

¿(D) section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) (to obtain certain financial information and consumer reports); and

¿(E) section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v) (to obtain credit agency consumer records for counterterrorism investigations).

¿(2) UNCLASSIFIED FORM.—The report under this section shall be submitted in unclassified form.

(c) REPORTS ON REQUESTS FOR NATIONAL SECURITY LETTERS.—

(1) DEFINITIONS.—In this subsection—

(A) the term "applicable period" means—

(i) with respect to the first report submitted under paragraph (2) or (3), the period beginning 180 days after the date of enactment of the USA PATRIOT Act Sunset Extension Act of 2011 and ending on December 31, 2011; and

(ii) with respect to the second report submitted under paragraph (2) or (3), and each report thereafter, the 6-month period ending on the last day of the second month before the date for submission of the report; and

(B) the term "United States person" has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(2) CLASSIFIED FORM.—

(A) IN GENERAL.—Not later than February 1, 2012, and every 6 months thereafter, the Attorney General shall submit to the Select Committee on Intelligence, the Committee on the Judiciary, and the Committee on Banking, Housing, and Urban Affairs of the Senate and the Permanent Select Committee on Intelligence, the Committee on the Judiciary, and the Committee on Financial Services of the House of Representatives a report fully informing the committees concerning the requests made under section 2709(a) of title 18, United States Code, section 1114(a)(5)(A) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(5)(A)), section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u), section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v), or section 802 of the National Security Act of 1947 (50 U.S.C. 436) during the applicable period.

(B) CONTENTS.—Each report under subparagraph (A) shall include, for each provision of law described in subparagraph (A)—

(i) the number of authorized requests under the provision, including requests for subscriber information; and

(ii) the number of authorized requests under the provision—

(I) that relate to a United States person;

(II) that relate to a person that is not a United States person;

(III) that relate to a person that is—

(aa) the subject of an authorized national security investigation; or

(bb) an individual who has been in contact with or otherwise directly linked to the subject of an authorized national security investigation; and

(IV) that relate to a person that is not known to be the subject of an authorized national security investigation or to have been in contact with or otherwise directly linked to the subject of an authorized national security investigation.

(3) UNCLASSIFIED FORM.—

(A) IN GENERAL.—Not later than February 1, 2012, and every 6 months thereafter, the Attorney General shall submit to the Select Committee on Intelligence, the Committee on the Judiciary, and the Committee on Banking, Housing, and Urban Affairs of the Senate and the Permanent Select Committee on Intelligence, the Committee on the Judiciary, and the Committee on Financial Services of the House of Representatives a report fully informing the committees concerning the aggregate total of all requests identified under paragraph (2) during the applicable period ending on the last day of the second month before the date for submission of the report. Each report under this subparagraph shall be in unclassified form.

(B) CONTENTS.—Each report under subparagraph (A) shall include the aggregate total of requests—

(i) that relate to a United States person;

(ii) that relate to a person that is not a United States person;

(iii) that relate to a person that is—

(I) the subject of an authorized national security investigation; or

(II) an individual who has been in contact with or otherwise directly linked to the subject of an authorized national security investigation; and

(iv) that relate to a person that is not known to be the subject of an authorized national security investigation or to have been in contact with or otherwise directly linked to the subject of an authorized national security investigation.

* * * * * * *

SEC. 119. AUDIT OF USE OF NATIONAL SECURITY LETTERS.

(a) AUDIT.—The Inspector General of the Department of Justice shall perform an audit of the effectiveness and use, including any improper or illegal use, of national security letters issued by the Department of Justice.

(b) REQUIREMENTS.—The audit required under subsection (a) shall include—

(1) an examination of the use of national security letters by the Department of Justice during calendar years 2003 through *2011* ¿2006 ;

(2) a description of any noteworthy facts or circumstances relating to such use, including any improper or illegal use of such authority; and

(3) an examination of the effectiveness of national security letters as an investigative tool, including—

(A) the importance of the information acquired by the Department of Justice to the intelligence activities of the Department of Justice or to any other department or agency of the Federal Government;

(B) the manner in which such information is collected, retained, analyzed, and disseminated by the Department of Justice, including any direct access to such information (such as access to "raw data") provided to any other department, agency, or instrumentality of Federal, State, local, or tribal governments or any private sector entity;

(C) whether, and how often, the Department of Justice utilized such information to produce an analytical intelligence product for distribution within the Department of Justice, to the intelligence community¿ (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4))) , or to other Federal, State, local, or tribal government departments, agencies, or instrumentalities;

(D) whether, and how often, the Department of Justice provided such information to law enforcement authorities for use in criminal proceedings;

(E) with respect to national security letters issued following the date of the enactment of this Act, an examination of the number of occasions in which the Department of Justice, or an officer or employee of the Department of Justice, issued a national security letter without the certification necessary to require the recipient of such letter to comply with the nondisclosure and confidentiality requirements potentially applicable under law; and

(F) the types of electronic communications and transactional information obtained through requests for information under section 2709 of title 18, United States Code, including the types of dialing, routing, addressing, or signaling information obtained, and the procedures the Department of Justice uses if content information is obtained through the use of such authority.

(c) SUBMISSION DATES.—

(1) PRIOR YEARS.—Not later than one year after the date of the enactment of this Act, or upon completion of the audit under this section for calendar years 2003 and 2004, whichever is earlier, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary and the Select Committee on Intelligence of the Senate a report containing the results of the audit conducted under this subsection for calendar years 2003 and 2004.

(2) CALENDAR YEARS 2005 AND 2006.—Not later than December 31, 2007, or upon completion of the audit under this subsection for calendar years 2005 and 2006, whichever is earlier, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary and the Select Committee on Intelligence of the Senate a report containing the results of the audit conducted under this subsection for calendar years 2005 and 2006.

(3) CALENDAR YEARS 2007, 2008, AND 2009.—Not later than March 31, 2012, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary and the Select Committee on Intelligence of the Senate a report containing the results of the audit conducted under this section for calendar years 2007, 2008, and 2009.

(4) CALENDAR YEARS 2010 AND 2011.—Not later than March 31, 2013, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary and the Select Committee on Intelligence of the Senate a report containing the results of the audit conducted under this section for calendar years 2010 and 2011.

(d) INTELLIGENCE ASSESSMENT.—

(1) IN GENERAL.—For the period beginning on January 1, 2007 and ending on December 31, 2011, the Inspector General of each element of the intelligence community outside of the Department of Justice that issued national security letters in the intelligence activities of the element of the intelligence community shall—

(A) examine the use of national security letters by the element of the intelligence community during the period;

(B) describe any noteworthy facts or circumstances relating to the use of national security letters by the element of the intelligence community, including any improper or illegal use of such authority;

(C) assess the importance of information received under the national security letters to the intelligence activities of the element of the intelligence community; and

(D) examine the manner in which information received under the national security letters was collected, retained, analyzed, and disseminated.

(2) SUBMISSION DATES FOR ASSESSMENT.—

(A) CALENDAR YEARS 2007 THROUGH 2009.—Not later than March 31, 2012, the Inspector General of each element of the intelligence community that conducts an assessment under this subsection shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives a report containing the results of the assessment for calendar years 2007 through 2009.

(B) CALENDAR YEARS 2010 AND 2011.—Not later than March 31, 2013, the Inspector General of any element of the intelligence community that conducts an assessment under this subsection shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives a report containing the results of the assessment for calendar years 2010 and 2011.

(e)¿(d) PRIOR NOTICE TO ATTORNEY GENERAL AND DIRECTOR OF NATIONAL INTELLIGENCE; COMMENTS.—

(1) NOTICE.—Not less than 30 days before the submission of *any report under subsection (c) or (d)*¿ a report under subsection (c)(1) or (c)(2) , the Inspector General of the Department of Justice *and any Inspector General of an element of the intelligence community that submits a report under this section* shall provide such report to the Attorney General and the Director of National Intelligence.

(2) COMMENTS.—The Attorney General or the Director of National Intelligence may provide comments to be included in ¿the reports submitted under subsection (c)(1) or (c)(2) *any report submitted under subsection (c) or (d)* as the Attorney General or the Director of National Intelligence may consider necessary.

(f)¿(e) UNCLASSIFIED FORM.—¿The reports submitted under subsection (c)(1) or (c)(2) *Each report submitted under subsection (c)*

and any comments included under *subsection (e)(2)* ¿subsection (d)(2) shall be in unclassified form, but may include a classified annex.

(g)¿(f) MINIMIZATION PROCEDURES FEASIBILITY.—Not later than February 1, 2007, or upon completion of review of the report submitted under subsection (c)(1), whichever is earlier, the Attorney General and the Director of National Intelligence shall jointly submit to the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary and the Select Committee on Intelligence of the Senate a report on the feasibility of applying minimization procedures in the context of national security letters to ensure the protection of the constitutional rights of United States persons.

¿(g) NATIONAL SECURITY LETTER DEFINED.—In this section, the term "national security letter" means a request for information under one of the following provisions of law:

¿(1) Section 2709(a) of title 18, United States Code (to access certain communication service provider records).

¿(2) Section 1114(a)(5)(A) of the Right to Financial Privacy Act (12 U.S.C. 3414(a)(5)(A)) (to obtain financial institution customer records).

¿(3) Section 802 of the National Security Act of 1947 (50 U.S.C. 436) (to obtain financial information, records, and consumer reports).

¿(4) Section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) (to obtain certain financial information and consumer reports).

¿(5) Section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v) (to obtain credit agency consumer records for counterterrorism investigations).

(h) DEFINITIONS.—In this section—

(1) the term "intelligence community" has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 401a);

(2) the term "national security letter" means a request for information under—

(A) section 2709(a) of title 18, United States Code (to access certain communication service provider records);

(B) section 1114(a)(5)(A) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(5)(A)) (to obtain financial institution customer records);

(C) section 802 of the National Security Act of 1947 (50 U.S.C. 436) (to obtain financial information, records, and consumer reports);

(D) section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) (to obtain certain financial information and consumer reports); or

(E) section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v) (to obtain credit agency consumer records for counterterrorism investigations); and

(3) the term "United States person" has the meaning given that term in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

* * * * * * *

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

PL 108–458 (118 Stat. 3742)

TITLE VI—TERRORISM PREVENTION

Subtitle A—Individual Terrorists as Agents of Foreign Powers

SEC. 6001. INDIVIDUAL TERRORISTS AS AGENTS OF FOREIGN POWERS.

* * * * * * *

¿(b) SUNSET.—The amendment made by subsection (a) shall be subject to the sunset provision in section 224 of Public Law 107–56 (115 Stat. 295), including the exception provided in subsection (b) of such section 224.

(b) SUNSET.—

(1) REPEAL.—Subparagraph (C) of section 101(b)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(b)(1)), as added by subsection (a), is repealed effective December 31, 2013.

(2) TRANSITION PROVISION.—Notwithstanding paragraph (1), subparagraph (C) of section 101(b)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(b)(1)) 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 particular offense that began or occurred before December 31, 2013.

* * * * * * *

FISA AMENDMENTS ACT OF 2008

Public Law No. 110–261

50 U.S.C. 1881 note

SEC. 403. REPEALS.

* * * * * * *

(b) FISA AMENDMENTS ACT OF 2008.—

(1) IN GENERAL.—Except as provided in section 404, effective *December 31, 2013* ¿December 31, 2012 , title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a), is repealed.

(2) TECHNICAL AND CONFORMING AMENDMENTS.—Effective *December 31, 2013* ¿December 31, 2012 —

(A) the table of contents in the first section of such Act (50 U.S.C. 1801 et seq.) is amended by striking the items related to title VII;

(B) except as provided in section 404, section 601(a)(1) of such Act (50 U.S.C. 1871(a)(1)) is amended to read as such section read on the day before the date of the enactment of this Act; and

(C) except as provided in section 404, section 2511(2)(a)(ii)(A) of title 18, United States Code, is amended by striking "or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978".

SEC. 404. TRANSITION PROCEDURES.

* * * * * * *

(b) TRANSITION PROCEDURES FOR FISA AMENDMENTS ACT OF 2008 PROVISIONS.—

(1) ORDERS IN EFFECT ON *DECEMBER 31, 2013* ¿DECEMBER 31, 2012 .—Notwithstanding any other provision of this Act, any amendment made by this Act, or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), any order, authorization, or directive issued or made under title VII of the Foreign Intelligence Surveillance Act of 1978, as amended by section 101(a), shall continue in effect until the date of the expiration of such order, authorization, or directive.

* * * * * * *

New Provisions Under USA PATRIOT Act

Sunset Extension Act of 2011 (S. 193)

SEC. 2.—SUNSETS.

* * * * * * *

(c) NATIONAL SECURITY LETTERS.—

(1) REPEAL.—Effective on December 31, 2013—

(A) section 2709 of title 18, United States Code, is amended to read as such provision read on October 25, 2001;

(B) section 1114(a)(5) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(5)) is amended to read as such provision read on October 25, 2001;

(C) subsections (a) and (b) of section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) are amended to read as subsections (a) and (b), respectively, of the second of the 2 sections designated as section 624 of such Act (15 U.S.C. 1681u) (relating to disclosure to the Federal Bureau of Investigation for counter-intelligence purposes), as added by Section 601 of the Intelligence Authorization Act for Fiscal year 1996 (Public Law 104–93; 109 Stat. 974), read on October 25, 2001; and

(D) section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v) is repealed; and (E) section 802 of the National Security Act of 1947 (50 U.S.C. 436) is amended to read as such provision read on October 25, 2001.

(2) TRANSITION PROVISION.—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.

(3) TECHNICAL AND CONFORMING AMENDMENTS.—Effective December 31, 2013—

(A) section 3511 of title 18, United States Code, is amended—

(i) in subsections (a), (c), and (d), by striking "or 627(a)" each place it appears; and

(ii) in subsection (b)(1)(A), as amended by section 6(b) of this Act, by striking "section 626 or 627 of the Fair Credit Reporting Act (15 U.S.C. 1681u and 1681v)" and inserting "section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u)";

(B) section 118(c) of the USA PATRIOT Improvement and Reauthorization Act of 2005 (18 U.S.C. 3511 note) is amended—

(i) in subparagraph (C), by adding "and" at the end;

(ii) in subparagraph (D), by striking "; and" and inserting a period; and

(iii) by striking subparagraph (E); and

(C) the table of sections for the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) is amended by striking the item relating to section 627.

SEC. 10.—AUDITS.

* * * * * * *

(c) PEN REGISTERS AND TRAP AND TRACE DEVICES.—

(1) AUDITS.—The Inspector General of the Department of Justice shall perform comprehensive audits of the effectiveness and use, including any improper or illegal use, of pen registers and trap and trace devices under title IV of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1841 et seq.) during the period beginning on January 1, 2007 and ending on December 31, 2011.

(2) REQUIREMENTS.—The audits required under paragraph (1) shall include—

(A) an examination of the use of pen registers and trap and trace devices under title IV of the Foreign Intelligence Surveillance Act of 1978 for calendar years 2007 through 2011;

(B) an examination of the installation and use of a pen register or trap and trace device on emergency bases under section 403 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1843);

(C) any noteworthy facts or circumstances relating to the use of a pen register or trap and trace device under title IV of the Foreign Intelligence Surveillance Act of 1978, including any improper or illegal use of the authority provided under that title; and

(D) an examination of the effectiveness of the authority under title IV of the Foreign Intelligence Surveillance Act of 1978 as an investigative tool, including—

(i) the importance of the information acquired to the intelligence activities of the Federal Bureau of Investigation;

(ii) the manner in which the information is collected, retained, analyzed, and disseminated by the Federal Bureau of Investigation, including any direct access to the information provided to any other department, agency, or instrumentality of Federal, State, local, or tribal governments or any private sector entity;

(iii) with respect to calendar years 2010 and 2011, an examination of the minimization procedures used in relation to pen registers and trap and trace devices under title IV of the Foreign Intelligence Surveillance Act of 1978 and whether the minimization procedures protect the constitutional rights of United States persons;

(iv) whether, and how often, the Federal Bureau of Investigation used information acquired under a pen register or trap and trace device under title IV of the Foreign Intelligence Surveillance Act of 1978 to produce an analytical intelligence product for distribution within the Federal Bureau of Investigation, to the intelligence community, or to another department, agency, or instrumentality of Federal, State, local, or tribal governments; and

(v) whether, and how often, the Federal Bureau of Investigation provided information acquired under a pen register or trap and trace device under title IV of the Foreign Intelligence Surveillance Act of 1978 to law enforcement authorities for use in criminal proceedings.

(3) SUBMISSION DATES.—

(A) PRIOR YEARS.—Not later than March 31, 2012, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives a report containing the results of the audit conducted under this section for calendar years 2007 through 2009.

(B) CALENDAR YEARS 2010 AND 2011.—Not later than March 31, 2013, the Inspector General of the Department of Justice shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives a report containing the results of the audit conducted under this section for calendar years 2010 and 2011.

(4) INTELLIGENCE ASSESSMENT.—

(A) IN GENERAL.—For the period beginning January 1, 2007 and ending on December 31, 2011, the Inspector Gen-

eral of any element of the intelligence community outside of the Department of Justice that used information acquired under a pen register or trap and trace device under title IV of the Foreign Intelligence Surveillance Act of 1978 in the intelligence activities of the element of the intelligence community shall—

(i) assess the importance of the information to the intelligence activities of the element of the intelligence community;

(ii) examine the manner in which the information was collected, retained, analyzed, and disseminated;

(iii) describe any noteworthy facts or circumstances relating to orders under title IV of the Foreign Intelligence Surveillance Act of 1978 as the orders relate to the element of the intelligence community; and

(iv) examine any minimization procedures used by the element of the intelligence community in relation to pen registers and trap and trace devices under title IV of the Foreign Intelligence Surveillance Act of 1978 and whether the minimization procedures protect the constitutional rights of United States persons.

(B) SUBMISSION DATES FOR ASSESSMENT.—

(i) CALENDAR YEARS 2007 THROUGH 2009.—Not later than March 31, 2012, the Inspector General of each element of the intelligence community that conducts an assessment under this paragraph shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives a report containing the results of the assessment for calendar years 2007 through 2009.

(ii) CALENDAR YEARS 2010 AND 2011.—Not later than March 31, 2013, the Inspector General of each element of the intelligence community that conducts an assessment under this paragraph shall submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representative a report containing the results of the assessment for calendar years 2010 and 2011.

(5) PRIOR NOTICE TO ATTORNEY GENERAL AND DIRECTOR OF NATIONAL INTELLIGENCE; COMMENTS.—

(A) NOTICE.—Not less than 30 days before the submission of any report under paragraph (3) or (4), the Inspector General of the Department of Justice and any Inspector General of an element of the intelligence community that submits a report under this susbsection shall provide the report to the Attorney General and the Director of National Intelligence.

(B) COMMENTS.—The Attorney General or the Director of National Intelligence may provide such comments to be included in any report submitted under paragraph (3) or (4)

as the Attorney General or the Director of National Intelligence may consider necessary.

(6) UNCLASSIFIED FORM.—Each report submitted under paragraph (3) and any comments included in that report under paragraph (5)(B) shall be in unclassified form, but may include a classified annex.

(d) DEFINITIONS.—In this section—

(1) the terms 'foreign intelligence information' and 'United States person' have the meanings given those terms in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801); and

(2) the term 'intelligence community' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 401a).

SEC. 12.—PROCEDURES.

(a) IN GENERAL.—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 issued under section 2709 of title 18, United States Code, section 1114(a)(5) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(5)), section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u), or section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v).

(b) CONSIDERATIONS.—In reviewing and revising the procedures described in subsection (a), the Attorney General shall give due consideration to the privacy interests of individuals and the need to protect national security.

(c) REVISIONS TO PROCEDURES AND OVERSIGHT.—If the Attorney General makes any significant changes to the procedures described in subsection (a), the Attorney General shall notify and submit a copy of the changes to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives.

APPENDIX

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 14, 2009

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Thank you for your letter requesting our recommendations on the three provisions of the Foreign Intelligence Surveillance Act ("FISA") currently scheduled to expire on December 31, 2009. We believe that the best legislation will emerge from a careful examination of these matters. In this letter, we provide our recommendations for each provision, along with a summary of the supporting facts and rationale. We have discussed these issues with the Office of the Director of National Intelligence, which concurs with the views expressed in this letter.

We also are aware that Members of Congress may propose modifications to provide additional protection for the privacy of law abiding Americans. As President Obama said in his speech at the National Archives on May 21, 2009, "We are indeed at war with al Qaeda and its affiliates. We do need to update our institutions to deal with this threat. But we must do so with an abiding confidence in the rule of law and due process; in checks and balances and accountability." Therefore, the Administration is willing to consider such ideas, provided that they do not undermine the effectiveness of these important authorities.

1. Roving Wiretaps, USA PATRIOT Act Section 206 (codified at 50 U.S.C. § 1805(c)(2))

We recommend reauthorizing section 206 of the USA PATRIOT Act, which provides for roving surveillance of targets who take measures to thwart FISA surveillance. It has proven an important intelligence-gathering tool in a small but significant subset of FISA electronic surveillance orders.

This provision states that where the Government sets forth in its application for a surveillance order "specific facts" indicating that the actions of the target of the order "may have the effect of thwarting" the identification, at the time of the application, of third parties necessary to accomplish the ordered surveillance, the order shall direct such third parties, when identified to furnish the Government with all assistance necessary to accomplish surveillance of the target identified in the order. In other words, the "roving" authority is only available when the Government is able to provide specific information that the target may engage in counter-surveillance activity (such as rapidly switching cell phone numbers. The language of the statute does not allow the Government to make a general, "boilerplate" allegation that the target may

engage in such activities; rather, the Government must provide specific facts to support its allegation.

There are at least two scenarios in which the Government's ability to obtain a roving wiretap may be critical to effective surveillance of a target. The first is where the surveillance targets a traditional foreign intelligence officer. In these cases, the Government often has years of experience maintaining surveillance of officers of a particular foreign intelligence service who are posted to locations within the United States. The FBI will have extensive information documenting the tactics and tradecraft practiced by officers of the particular intelligence service, and may even have information about the training provided to those officers in their home country. Under these circumstances, the Government can represent that an individual who has been identified as an officer of that intelligence service is likely to engage in counter-surveillance activity.

The second scenario in which the ability to obtain a roving wiretap may be critical to effective surveillance is the case of an individual who actually has engaged in counter-surveillance activities or in preparations for such activities. In some cases, individuals already subject to FISA surveillance are found to be making preparations for counter-surveillance activities or instructing associates on how to communicate with them through more secure means. In other cases, non-FISA investigative techniques have revealed counter-surveillance preparations (such as buying "throwaway" cell phones or multiple calling cards). The Government then offers these specific facts to the FISA court as justification for a grant of roving authority.

Since the roving authority was added to FISA in 2001, the Government has sought to use it in a relatively small number of cases (on average, twenty-two applications a year). We would be pleased to brief Members or staff regarding actual numbers, along with specific case examples, in a classified setting. The FBI uses the granted authority only when the target actually begins to engage in counter-surveillance activity that thwarts the already authorized surveillance, and does so in a way that renders the use of roving authority feasible.

Roving authority is subject to the same court-approved minimization rules that govern other electronic surveillance under FISA and that protect against the unjustified acquisition or retention of non-pertinent information. The statute generally requires the Government to notify the FISA court within 10 days of the date upon which surveillance begins to be directed at any new facility. Over the past seven years, this process has functioned well and has provided effective oversight for this investigative technique.

We believe that the basic justification offered to Congress in 2001 for the roving authority remains valid today. Specifically, the ease with which individuals can rapidly shift between communications providers, and the proliferation of both those providers and the services they offer, almost certainly will increase as technology continues to develop. International terrorists, foreign intelligence officers, and espionage suspects — like ordinary

criminals — have learned to use these numerous and diverse communications options to their advantage. Any effective surveillance mechanism must incorporate the ability to rapidly address an unanticipated change in the target's communications behavior. The roving electronic surveillance provision has functioned as intended and has addressed an investigative requirement that will continue to be critical to national security operations. Accordingly, we recommend reauthorizing this feature of FISA.

2. "Business Records," USA PATRIOT Act Section 215 (codified at 50 U.S.C. § 1861-62)

We also recommend reauthorizing section 215 of the USA PATRIOT Act, which allows the FISA court to compel the production of "business records." The business records provision addresses a gap in intelligence collection authorities and has proven valuable in a number of contexts.

The USA PATRIOT Act made the FISA authority relating to business records roughly analogous to that available to FBI agents investigating criminal matters through the use of grand jury subpoenas. The original FISA language, added in 1998, limited the business records authority to four specific types of records, and required the Government to demonstrate "specific and articulable facts" supporting a reason to believe that the target was an agent of a foreign power. In the USA PATRIOT Act, the authority was changed to encompass the production of "any tangible things" and the legal standard was changed to one of simple relevance to an authorized investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

The Government first used the USA PATRIOT Act business records authority in 2004 after extensive internal discussions over its proper implementation. The Department's inspector general evaluated the Department's implementation of this new authority at length, in reports that are now publicly available. Other parts of the USA PATRIOT Act, specifically those eliminating the "wall" separating intelligence operations and criminal investigations, also had an effect on the operational environment. The greater access that intelligence investigators now have to criminal tools (such as grand jury subpoenas) reduces but does not eliminate the need for intelligence tools such as the business records authority. The operational security requirements of most intelligence investigations still require the secrecy afforded by the FISA authority.

For the period 2004-2007, the FISA court has issued about 220 orders to produce business records. Of these, 173 orders were issued in 2004-06 in combination with FISA pen register orders to address an anomaly in the statutory language that prevented the acquisition of subscriber identification information ordinarily associated with pen register information. Congress corrected this deficiency in the pen register provision in 2006 with language in the USA PATRIOT Improvement and Reauthorization Act. Thus, this use of the business records authority became unnecessary.

The remaining business records orders issued between 2004 and 2007 were used to obtain transactional information that did not fall within the scope of any other national security investigative authority (such as a national security letter). Some of these orders were used to support important and highly sensitive intelligence collection operations, of which both Members of the Intelligence Committee and their staffs are aware. The Department can provide additional information to Members or their staff in a classified setting.

It is noteworthy that no recipient of a FISA business records order has ever challenged the validity of the order, despite the availability, since 2006, of a clear statutory mechanism to do so. At the time of the USA PATRIOT Act, there was concern that the FBI would exploit the broad scope of the business records authority to collect sensitive personal information on constitutionally protected activities, such as the use of public libraries. This simply has not occurred, even in the environment of heightened terrorist threat activity. The oversight provided by Congress since 2001 and the specific oversight provisions added to the statute in 2006 have helped to ensure that the authority is being used as intended.

Based upon this operational experience, we believe that the FISA business records authority should be reauthorized. There will continue to be instances in which FBI investigators need to obtain transactional information that does not fall within the scope of authorities relating to national security letters and are operating in an environment that precludes the use of less secure criminal authorities. Many of these instances will be mundane (as they have been in the past), such as the need to obtain driver's license information that is protected by State law. Others will be more complex, such as the need to track the activities of intelligence officers through their use of certain business services. In all these cases, the availability of a generic, court-supervised FISA business records authority is the best option for advancing national security investigations in a manner consistent with civil liberties. The absence of such an authority could force the FBI to sacrifice key intelligence opportunities.

3. "Lone Wolf," Intelligence Reform and Terrorism Prevention Act of 2004 Section 6001 (codified at 50 U.S.C. § 1801(b)(1)(C))

Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004 defines a "lone wolf" agent of a foreign power and allows a non-United States person who "engages in international terrorism activities" to be considered an agent of a foreign power under FISA even though the specific foreign power (*i.e.*, the international terrorist group) remains unidentified. We also recommend reauthorizing this provision.

Enacted in 2004, this provision arose from discussions inspired by the Zacarias Moussaoui case. The basic idea behind the authority was to cover situations in which information linking the target of an investigation to an international group was absent or insufficient, although the target's engagement in "international terrorism" was sufficiently established. The definition is quite narrow: it applies only to non-United States persons; the activities of the person must meet the FISA definition of "international terrorism;" and the

information likely to be obtained must be foreign intelligence information. What this means, in practice, is that the Government must know a great deal about the target, including the target's purpose and plans for terrorist activity (in order to satisfy the definition of "international terrorism"), but still be unable to connect the individual to any group that meets the FISA definition of a foreign power.

To date, the Government has not encountered a case in which this definition was both necessary and available, *i.e.*, the target was a non-United States person. Thus, the definition has never been used in a FISA application. However, we do not believe that this means the authority is now unnecessary. Subsection 101(b) of FISA provides ten separate definitions for the term "agent of a foreign power" (five applicable only to non-United States persons, and five applicable to all persons). Some of these definitions cover the most common fact patterns; others describe narrow categories that may be encountered rarely. However, this latter group includes legitimate targets that could not be accommodated under the more generic definitions and would escape surveillance but for the more specific definitions.

We believe that the "lone wolf" provision falls squarely within this class. While we cannot predict the frequency with which it may be used, we can foresee situations in which it would be the only avenue to effective surveillance. For example, we could have a case in which a known international terrorist affirmatively severed his connection with his group, perhaps following some internal dispute. The target still would be an international terrorist, and an appropriate target for intelligence surveillance. However, the Government could no longer represent to the FISA court that he was currently a member of an international terrorist group or acting on its behalf. Lacking the "lone wolf" definition, the Government could have to postpone FISA surveillance until the target could be linked to another group. Another scenario is the prospect of a terrorist who "self-radicalizes" by means of information and training provided by a variety of international terrorist groups via the Internet. Although this target would have adopted the aims and means of international terrorism, the target would not actually have contacted a terrorist group. Without the lone wolf definition, the Government might be unable to establish FISA surveillance.

These scenarios are not remote hypotheticals; they are based on trends we observe in current intelligence reporting. We cannot determine how common these fact patterns will be in the future or whether any of the targets will so completely lack connections to groups that they cannot be accommodated under other definitions. However, the continued availability of the lone wolf definition eliminates any gap. The statutory language of the existing provision ensures its narrow application, so the availability of this potentially useful tool carries little risk of overuse. We believe that it is essential to have the tool available for the rare situation in which it is necessary rather than to delay surveillance of a terrorist in the hopes that the necessary links are established.

Thank you for the opportunity to present our views. We would be happy to meet with your staff to discuss them. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

Ronald Weich
Assistant Attorney General

cc: The Honorable Jeff Sessions
Ranking Minority Member

Office of the Attorney General
Washington, D.C. 20530

November 9, 2009

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

The Honorable Dianne Feinstein
Chairman
Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

Dear Chairman Leahy and Chairman Feinstein:

I am writing to express the strong support of the Department of Justice for S. 1692, the USA PATRIOT Act Sunset Extension Act, as reported by the Judiciary Committee.

This legislation reauthorizes several important authorities in the Foreign Intelligence Surveillance Act ("FISA"), including the authority for roving surveillance of targets who take steps to thwart FISA surveillance, the authority to compel production of business records and other tangible things with approval of the FISA court, and the authority to target with FISA surveillance non-United States persons who engage in international terrorist activities but are not necessarily associated with an identified terrorist group. For reasons expressed in the Department's September 14 letter to Chairman Leahy, we believe these authorities are critical to national security investigations, and we are pleased that the pending legislation comports with our recommendation that they be renewed.

We are also pleased that S. 1692 includes a number of provisions designed to enhance statutory protections for civil liberties and privacy in the exercise of these and related authorities. These include the following: authorization for court-imposed minimization requirements for information obtained via pen register or trap and trace orders in exceptional cases; judicial oversight of the Government's compliance with business record and pen register or trap and trace minimization procedures; heightened standards for use of the business records authority to obtain library circulation records and patron lists; the elimination of a waiting period before nondisclosure requirements for business records orders can be challenged in court, and the elimination of the conclusive effect of the Government's certification of the need for non-disclosure; as well as inspector general audits of use of these authorities. We believe these measures will promote appropriate standards, oversight, and accountability, especially with respect to how information about United States persons is retained and disseminated, without sacrificing the operational effectiveness and flexibility of the underlying tools needed to protect

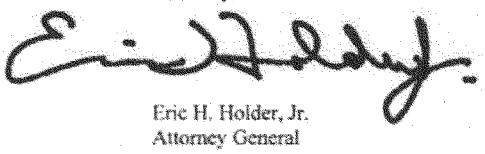
our citizens from terrorism and to facilitate the collection of vital foreign intelligence and counterintelligence information.

We also support additional civil liberties protections included in the bill with regard to national security letters ("NSLs"), which remain a critical tool of national security investigations. These protections include provisions that make clear that the recipient of an NSL nondisclosure order may challenge the order at any time, put the burden on the Government to initiate judicial review, eliminate the conclusive effect of the Government's certification on the need for nondisclosure, and require the Government to notify any recipient of an order who has objected to nondisclosure if and when the requirement for nondisclosure no longer exists. These changes are designed to satisfy the requirements of the Second Circuit Court of Appeal's decision in *Doe v. Mukasey*, 549 F.3d 861 (2d. Cir. 2008). The bill also will require the FBI, consistent with current practice, to prepare and retain a statement of the facts indicating that the information sought via NSL is relevant to an authorized national security investigation and will call for additional inspector general audits of the use of NSLs. We believe these requirements reflect appropriate checks and balances on the Government's use of this important authority.

While we are very pleased to be able to support the bill, we do have some concerns that we are working with the Committee to address before the measure reaches the floor. In particular, we are working with the Committee on provisions regarding procedures for the collection, use, and storage of information obtained through NSLs; certain public reporting and audit requirements; and provisions to ensure a smooth transition to the new law.

Thank you for the opportunity to present our views. The Office of Management and Budget has advised us that, from the standpoint of the Administration's program, there is no objection to the submission of this letter.

Sincerely,



Eric H. Holder, Jr.
Attorney General

cc: The Honorable Jeff Sessions
Committee on the Judiciary
United States Senate

The Honorable Christopher S. Bond
Vice Chairman
Select Committee on Intelligence
United States Senate

The Honorable Harry Reid
Majority Leader
United States Senate
Washington, D.C. 20510

February 19, 2010

The Honorable Nancy Pelosi
Speaker
United States House of Representatives
Washington, D.C. 20515

Dear Majority Leader Reid and Speaker Pelosi:

Over the past several months, Congress has been considering the reauthorization of three important provisions of the Foreign Intelligence Surveillance Act (FISA), which are scheduled to expire on February 28, 2010: section 206 of the USA PATRIOT Act, which provides authority for roving surveillance of targets who take steps to thwart FISA surveillance; section 215 of the USA PATRIOT Act, which provides authority to compel production of business records and other tangible things with the approval of the FISA court; and section 6001 of the Intelligence Reform and Terrorism Prevention Act, which provides authority to target with FISA surveillance non-United States persons who engage in international terrorist activities but are not necessarily associated with an identified terrorist group. National security requires that these provisions be reauthorized before they expire.

As discussed in the Attorney General's November 9, 2009 letter, we believe that S. 1692, the USA PATRIOT Act Sunset Extension Act, as reported by the Senate Judiciary Committee, strikes the right balance by both reauthorizing these essential national security tools and enhancing statutory protections for civil liberties and privacy in the exercise of these and related authorities. We were very pleased that the bill received bipartisan support in the Committee.

Since the bill was reported, we have negotiated a number of specific changes with the sponsors of the bill which we support including in the final version of this legislation. Among these are several provisions derived from the bills reported by the House Judiciary Committee and introduced by House Permanent Select Committee on Intelligence Chairman Silvestre Reyes in November.

We strongly support the prompt consideration of USA PATRIOT Act reauthorization legislation based on S. 1692, together with the changes to which our staffs have informally agreed. However, if Congress is unable to complete work on this measure before these authorities expire, it is imperative that Congress pass a temporary extension of sufficient length to ensure that there is no disruption to the availability of these vital tools in the fight against terrorists.

As was previously noted in a September 14 letter from the Department of Justice to Senator Patrick Leahy, the business records authority has been used to support important and highly sensitive intelligence collection operations, of which both Senate and House leadership, as well as Members of the Intelligence and Judiciary Committees and their staffs are aware. We can provide additional information to Members concerning these and related operations in a classified setting.

Finally, we remain committed to working with Congress to examine additional ways to enhance protection for civil liberties and privacy consistent with effective use of these important authorities.

The Office of Management and Budget has advised us that there is no objection to this letter from the perspective of the Administration's program.

Sincerely,

Eric H. Holder Jr.

Dennis C. Blair

United States Senate

COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6275

March 17, 2010

The Honorable Glenn A. Fine
Inspector General
United States Department of Justice
950 Pennsylvania Ave, N.W.
Washington, D.C. 20530

Dear Inspector General Fine:

Congress recently passed legislation extending, until February 28, 2011, three authorities of the Foreign Intelligence Surveillance Act of 1978 (FISA) that were due to sunset on December 31, 2009 pursuant to the USA PATRIOT Improvement and Reauthorization Act of 2005 (PATRIOT Act). These are sections 206 and 215 of the PATRIOT Act, and section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004. As you know, this temporary one-year extension does not include the improvements of existing law that were included in the bipartisan bill reported by the Senate Judiciary Committee last October, the USA PATRIOT Act Sunset Extension Act, S.1692, or the improvements negotiated in November and December of last year and endorsed by the Administration. We had sought to preserve important intelligence tools while promoting transparency, accountability, and civil liberties. In my view, it would be a mistake to wait yet another year before the Administration implements these reforms.

The 2008 Inspector General audit on National Security Letters, as well as the follow-up report on the abuse of exigent letters, detailed the previous abuse of these authorities by the FBI, and were essential to understanding how this power was being misused. Your office has also conducted comprehensive audits of section 215 orders. These audits represent a significant portion of the public reporting on the use of surveillance authorities and are a critical oversight tool over these authorities. As you said during your testimony before the Senate Judiciary Committee last year on reauthorizing these three PATRIOT Act provisions, the Inspector General's office "has an important role to play in the oversight process." I agree, and I believe we should not delay in exercising that role.

Please proceed to perform the audits of the use of section 215 orders, pen register and trap and trace devices, and National Security Letters (NSLs) included in S.1692, and submit reports no later than September 30, 2011, for the period covering calendar years 2007 through 2009, and no later than December 31, 2012, for calendar years 2010 and 2011. I worked with Senator Feinstein, who is a member of the Judiciary Committee and also the Chair of the Senate Select Committee on Intelligence, to require that the relevant Inspectors General of the intelligence community conduct their own audits of these provisions in a manner consistent with the audits that would be conducted by your office. I would encourage you to work with the Inspectors General of the intelligence community to ensure their participation and cooperation with respect to your investigations.

Sincerely,

PATRICK J. LEAHY
Chairman

Enclosure

United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6275

March 17, 2010

The Honorable Eric H. Holder, Jr.
Attorney General
United States Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20001

Dear Attorney General Holder:

Congress recently passed legislation extending, until February 28, 2011, three authorities of the Foreign Intelligence Surveillance Act of 1978 (FISA) that were due to sunset on December 31, 2009 pursuant to the USA PATRIOT Improvement and Reauthorization Act of 2005 (PATRIOT Act). These are sections 206 and 215 of the PATRIOT Act, and section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004. As you know, this temporary one-year extension does not include the improvements of existing law that were included in the bipartisan bill reported by the Senate Judiciary Committee last October, the USA PATRIOT Act Sunset Extension Act, S.1692, negotiated in November and December of last year, and endorsed by the Administration. We had sought to preserve important intelligence tools while promoting transparency, accountability, and civil liberties. In my view, it would be a mistake to wait yet another year before the Administration implements these reforms.

Last November 9, 2009, you sent a letter strongly endorsing the reported bill and expressing the Department of Justice's support for the expanded privacy and civil liberties protections it contained. The letter also stated unequivocally that the changes to law contained in the bill pose no operational concerns. In response to a few outstanding concerns of the Department, I negotiated a manager's amendment that also received the support of the Administration. Last December, I worked with Senate and House leadership to reach agreement with respect to additional improvements, including new reporting requirements on the use of section 215 orders and a mandate that Congress be notified when the so-called "lone wolf" provision is used. On February 19, 2010, the Department of Justice sent Senate and House leadership a letter urging passage of S.1692, including the modifications that had been subsequently negotiated. The letter acknowledges that the bill "strikes the right balance by both reauthorizing these essential national security tools and enhancing statutory protections for civil liberties and privacy...."

The one-year extension should not become an excuse to defer implementation of the important civil liberties and enhanced accountability provisions of S.1692 and subsequent negotiations that received the support of the Administration. We should work together to ensure that these important accountability provisions are realized without delay. A number of the improvements that were included in the bill should not require statutory changes. Even without congressional action the Administration can issue the reports that were included in the Senate bill as well as those negotiated between the Senate and House leadership. These reports would be in addition to those that are currently required by statute, and would include increased public reporting on the use of National Security Letters (NSLs), an annual unclassified report on the use of FISA authorities and the impact on the privacy of U.S. persons, and a public report detailing ways in which the Government can exercise its section 215 authority while providing enhanced protections for civil liberties. To the extent consistent with classification requirements, all of these reports could be posted on the Department of Justice website so that the public has the opportunity to learn more about how these authorities are being used.

As you know, a key measure in S.1692 aimed at increasing accountability was a new sunset for National Security Letters (NSLs). For years, I have been concerned about the issuance and oversight of NSLs. We now know that the National Security Letter authority was significantly misused. That is why I fought hard to retain a sunset for National Security Letters in our legislation, in addition to an audit. It is important that there be increased accountability for this authority. I urge you to proceed without delay to implement the accountability measures that were in our bill with respect to NSLs. Some improvements can be achieved through the issuance of internal policies, procedures, and guidance. Last September, FBI Director Mueller testified before the Judiciary Committee that the FBI had already instituted nationwide changes to its procedures for seeking nondisclosure orders on National Security Letters – a constitutional fix that we sought to codify with the Senate legislation. I applaud the FBI's efforts to rectify this constitutional deficiency proactively, and would like to receive specific information about how these new procedures have been implemented around the country. Please inform the Committee when and how the FBI will implement procedures related to the collection, use, and storage of information obtained in response to a National Security Letters, and how the procedures will be enforced.

Similarly, while I am encouraged by the progress the FBI has made in reforming its system for issuing and monitoring National Security Letters, the FBI should issue formal policies for retaining internally a statement of specific facts showing that the information sought is relevant to an authorized investigation. This information would be available for internal review and audits, and the development of formal policy guidance governing this practice would be simple, yet important, progress. A further improvement in the legislation that the administration should undertake is to require the FBI to notify NSL recipients who challenge nondisclosure orders when compliance with the order is no longer required.

I also plan to request that the Department of Justice Inspector General conduct the audits that were included in S.1692. The importance of these types of audits was underscored by the Department of Justice Inspector General's 2008 NSL audit, as well as the follow-up report on the abuse of exigent letters, both of which detailed the previous abuse of this significant authority. If we are to afford the Government these broad authorities, it is critical that there be significant oversight with respect to how they are being used.

I am also asking for your cooperation in determining how we can move forward in implementing the policies and procedures that achieve the goals of the legislation. With regard to section 215 orders, please explain the policy guidance you will issue in order to realize the changes to section 215 orders that you supported in the bill, including the additional provisions negotiated in December. For example, there is no reason that the Government should be afforded a presumption in its favor when it is asking the court to issue a section 215 order. Assistant Attorney General for National Security David Kris acknowledged during a Senate Judiciary Committee hearing on this issue last year that, in order to obtain such an order from the Foreign Intelligence Surveillance Court (FISC) the Government must, "establish reasonable grounds to believe that the documents are relevant." I urge you to issue guidance that requires the FBI to present the FISC with a complete statement of facts sufficient to show relevance of the section 215 order to an authorized investigation. In instances where the Government is seeking to obtain section 215 records that contain bookseller records, or records from a library and contain personally identifiable information about a patron of the library, I urge you to issue guidance requiring the Government to meet the higher standard for section 215 records that was negotiated in December.

Furthermore, with regard to the issuance of orders preventing the disclosure of requests for material pursuant to section 215, the Government does not need the conclusive presumption in its favor when it asserts a potential danger to national security or interference with diplomatic relations. Accordingly, I encourage you to issue guidance that requires certifications accompanying applications for section 215 nondisclosure orders to include an appropriately thorough statement of facts that sets forth the need for nondisclosure.

Another provision in S.1692 that you supported would require court-approved minimization procedures for both section 215 orders and pen register and trap and trace devices. Please explain how you will institute appropriate guidelines that are consistent with the intent of the bill in this regard, and whether you will seek the approval of the FISC prior to implementing the provisions.

I share your concern that our Government be provided with the tools it needs to protect our national security. I also know that you share my commitment to ensuring that these sweeping authorities are being used responsibly and not unnecessarily infringing upon our citizens' civil liberties. I look forward to the Department's action and ideas so that we can work together on these matters now, without delay.

Sincerely,

PATRICK LEAHY
Chairman

U.S. Department of Justice

Office of the Inspector General

June 15, 2010

The Honorable Patrick J. Leahy
Chairman, Committee on the Judiciary
United States Senate
433 Russell Senate Building
Washington, D.C. 20510

Dear Mr. Chairman:

This is in response to your letter dated March 17, 2010, concerning provisions in the USA PATRIOT Act Sunset Extension Act of 2009, S.1692, that would have required the Department of Justice Office of the Inspector General (OIG) and other Inspectors General in the intelligence community to conduct reviews of certain authorities contained in the Foreign Intelligence Surveillance Act of 1978 (FISA).

In your letter, you asked the OIG to conduct a review addressing these provisions, even though that bill was not enacted. We are writing this letter to inform you that the OIG is initiating a review that is intended to examine many of these provisions.

As you are aware, the OIG's March 2007 and March 2008 reports on the Federal Bureau of Investigation's (FBI) use of national security letters (NSLs) and Section 215 orders for business records made a total of 31 recommendations to improve the FBI's use of these authorities and ensure the FBI's compliance with the requirements governing their use. In addition, in January 2010 we completed our report on the FBI's use of exigent letters and other informal requests, instead of national security letters or other legal process, to obtain the production of non-content telephone records. In that report, we made 13 additional recommendations to address deficiencies we identified in the FBI's compliance with the statutes, guidelines, regulations, and policies governing the FBI's authority to request and obtain telephone records.

We intend to initiate another review examining the FBI's use of NSLs and Section 215 orders for business records. Among other issues, our review will assess the FBI's progress in responding to the OIG's recommendations in the prior reports. In addition, we intend to examine the number of NSLs issued by the FBI from 2007 through 2009, and we will closely examine the automated

system to generate and track NSLs that the FBI implemented to address the deficiencies identified in the OIG reports.

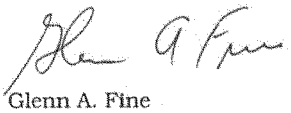
In addition, our review will cover the FBI's use of Section 215 orders for business records. It will examine the number of Section 215 applications filed from 2007 through 2009, how the FBI is using the tool today, and describe any reported improper or illegal uses of the authority. Our review also will examine the progress the FBI has made in addressing recommendations contained in our prior reports that the FBI draft and implement minimization procedures specifically for information collected under Section 215 authority.

We also intend to conduct a programmatic review of the FBI's use of its pen register and trap and trace authority under the FISA. That part of the review will examine issues such as how the FBI uses this authority to collect information, what the FBI does with the information it collects, and whether there have been any improper or illegal uses of the authority either reported by the FBI or identified by the OIG.

Thus, while our review may not address every one of the specific provisions that were contained in Senate Bill 1692, we anticipate that the results of our review will address many of the important issues reflected in the oversight provisions that were part of that bill.

If you have any questions about this letter or these issues, please contact me or Cynthia Schnedar from my office at (202) 514-3435.

Sincerely,



Glenn A. Fine
Inspector General

cc: Honorable Jeff Sessions
Ranking Member
Committee on the Judiciary

Office of the Attorney General
Washington, D. C. 20530

December 9, 2010

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Chairman Leahy:

This responds to your letter of March 17, 2010, which asked the Department of Justice to consider implementing administratively certain enhanced civil liberties protections that were included in S. 1692, the USA PATRIOT Act Sunset Extension Act, as reported by the Senate Judiciary Committee.

In my letter of November 9, 2009, I expressed strong support on behalf of the Department for the bill as reported, which would reauthorize several important Foreign Intelligence Surveillance Act (FISA) authorities while enhancing protections for civil liberties and privacy in the exercise of these essential national security tools.

The bill would reauthorize section 206 of the USA PATRIOT Act, which provides authority for roving surveillance of targets who take steps that thwart FISA surveillance; section 215 of the USA PATRIOT Act, which provides authority to compel production of business records and other tangible things with the approval of the Foreign Intelligence Surveillance Court (the FISA Court); and section 6001 of the Intelligence Reform and Terrorism Prevention Act, which provides authority to target with FISA searches or surveillance non-United States persons who engage in international terrorist activities but are not necessarily associated with an identified terrorist group. Earlier this year, Congress acted to extend the expiring authorities until February 28, 2011. As that date approaches, I strongly urge that Congress again take action to ensure that these provisions remain in force.

Assuming these authorities are reauthorized, the Department has determined that many of the privacy and civil liberties provisions of S. 1692 can be implemented without legislation. Indeed, in a number of instances, we have already taken steps to do so. I am confident that these measures will enhance standards, oversight, and accountability, especially with respect to how information about U.S. persons is retained and disseminated, without sacrificing the operational effectiveness and flexibility needed to protect our citizens from terrorism and facilitate the collection of vital foreign intelligence and counterintelligence information.

National Security Letters

Your letter seeks our response regarding several matters related to National Security Letters (NSLs): notification to recipients of NSLs of their opportunity to contest the nondisclosure requirement; issuance of procedures related to the collection, use and storage of information obtained in response to NSLs; retention of a statement of specific facts that the information sought is relevant to an authorized investigation; and increased public reporting on the use of NSLs.

You will be pleased to know that as of February 2009, all NSLs are required to include a notice that informs recipients of the opportunity to contest the nondisclosure requirement through the government initiated judicial review. In most cases, this notice is automatically generated by the NSL subsystem. Domestic Investigations and Operations Guide (DIOG) § 11.9.3.E. The FBI also will ensure that in any case in which a recipient challenges a nondisclosure order, the recipient is notified when compliance with the order is no longer required. Thus far, there have been only four challenges to the non-disclosure requirement, and in two of the challenges, the FBI permitted the recipient to disclose the fact that an NSL was received. If and when the volume of such requests becomes sufficiently large that solutions beyond "one-off" notifications are required, the FBI will develop appropriate policies and procedures to notify the recipient when non-disclosure is no longer required.

I also am pleased to report that I approved Procedures for the Collection, Use and Storage of Information Derived from National Security Letters on October 1, 2010, and these procedures have been provided to the Judiciary and Intelligence Committees. The 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 will shortly complete work on a joint report to Congress on NSL "minimization" as required by the PATRIOT Reauthorization Act of 2005.

As to the information retained internally in connection with the issuance of NSLs, it is current policy for the FBI to retain a statement of specific facts showing that the information sought through NSLs is relevant to an authorized investigation. DIOG § 11.9.3.C.

The Department appreciates the desire of the Committee for enhanced public reporting on the use of NSLs. Accordingly, although the FBI cannot provide information regarding subcategories of NSLs in a public setting, it will continue to report publicly the aggregate numbers of NSLs on an annual basis and will evaluate whether any additional information can be publicly reported.

Section 215 Orders

Your letter also raises a number of matters related to section 215 orders. You seek assurances that the government will not rely on the conclusive presumption in section 215 and will present the FISA Court with a complete statement of facts sufficient to show relevance of the tangible things requested to an authorized investigation. It is current FBI practice to provide the Foreign Intelligence Surveillance Court with a complete statement of facts to support issuance of an order. The FBI is reviewing the DIOG to determine whether changes need to be made to reflect this practice. With respect to section 215 records that contain bookseller records, or are from a library and contain personally identifiable information about a patron of the library, we are prepared to require a statement of specific and articulable facts as would have been required under S. 1692, and to notify Congress should it become necessary to change that practice.

You ask the Department to issue policy guidance providing that certifications accompanying applications for section 215 nondisclosure orders must include an appropriately thorough statement of facts that sets forth the need for nondisclosure. I am pleased to report that this is current FBI practice, and the FBI is reviewing the DIOG to determine whether revisions should be made to reflect this practice.

You also ask the Department to institute guidelines to require court-approved minimization procedures for section 215 orders and pen register and trap and trace (PR/TT) devices. Minimization procedures are already required by statute in relation to section 215 orders. 50 USC § 1861(b)(2)(B). The proposal to extend this requirement to PR/TT orders is intended to apply only to certain intelligence collection activities. Procedures governing these operations are currently in effect, having been proposed by the government and approved by the FISA Court.

Finally, you ask the Department to consider providing an annual unclassified report on the use of FISA authorities and the impact on privacy of United States persons. I believe that providing greater transparency regarding the U.S. government's exercise of FISA authorities is an important objective, and will show the care taken by officials to implement and comply with constitutional and statutory requirements to protect the privacy of United States persons. Although the Department has concerns that there may be little additional information that can be provided in an unclassified format and that such unclassified information could be unintentionally misleading, we are prepared to work with the committee and our partners in the Intelligence Community to determine whether there is a way to overcome these difficulties and make additional information publicly available regarding the use of these authorities.

Taken together, I believe these measures will advance the goals of S. 1692 by enhancing the privacy and civil liberties our citizens enjoy without compromising our ability to keep our nation safe and secure.

I hope this information is helpful. The Department stands ready to work with Congress to ensure that the expiring FISA authorities are reauthorized in a timely way.

Sincerely,

Eric H. Holder, Jr.
Attorney General

cc: Honorable Jeff Sessions
Ranking Republican Member