AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 177

111TH CONGRESS, *1st Session* | SENATE | REPORT 111–92

THE USA PATRIOT ACT SUNSET EXTENSION ACT OF 2009

OCTOBER 28, 2009.—Ordered to be printed

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

R E P O R T

together with

ADDITIONAL AND MINORITY VIEWS

[To accompany S. 1692]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to which was referred the bill (S. 1692), 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 an amendment, and recommends that the bill, as amended, do pass.

CONTENTS

		Page
I.	Background and Purpose of The USA PATRIOT Act Sunset Extension Act of 2009	1
II.	History of the Bill and Committee Consideration	3
III.	Section-by-Section Summary of the Bill	7
IV.	Congressional Budget Office Cost Estimate	10
V.	Regulatory Impact Evaluation	11
VI.	Conclusion	11
VII.	Additional and Minority Views	13
VIII.	Changes to Existing Law Made by the Bill, as Reported	33

I. BACKGROUND AND PURPOSE OF THE USA PATRIOT ACT SUNSET EXTENSION ACT OF 2009

Congress acted swiftly after the September 11, 2001, attacks to pass the USA PATRIOT Act and to provide the Government with

89–010

the tools necessary to pursue terrorists and others that would do harm to our country. In order to ensure that the increased information-gathering powers of the Government would be implemented appropriately, however, Congress also included in the USA PATRIOT Act additional oversight measures and sunsets on some of the surveillance authorities with the greatest potential to impact U.S. citizens.

During the 109th Congress, a number of the expiring provisions of the 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 USA PATRIOT Act, which authorized "roving" wiretaps and orders for business records under the Foreign Surveillance Intelligence Act (FISA). The "lone wolf" authority under FISA was also viewed as controversial by some. Accordingly, the USA PATRIOT Improvement and Reauthorization Act of 2005 included a new sunset of December 31, 2009 for these three provisions. The USA PATRIOT Improvement and Reauthorization Act of 2005 also mandated that the Department of Justice, Office of Inspector General complete comprehensive audits on the Government's use of national security letters (NSLs) and requests for production of business records under section 215 of the 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, and found numerous instances of over-collection of information. In reports on the use of NSLs, the Inspector General cited faulty recordkeeping, poor tracking systems, and both misuse and abuse of the NSL authority.

The USA PATRIOT Act Sunset Extension Act of 2009, S. 1692, as amended and reported by the Committee, and as described more fully below, strikes a reasonable balance between the Government's need to maintain the tools necessary for effective counterterrorism investigations with the civil liberties and constitutional protections 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 the "lone wolf" provision. It also imposes a new four-year sunset on the use of NSLs. As set forth more fully below, the bill also strengthens oversight and judicial review, and addresses constitutional concerns about NSL nondisclosure orders raised by the Court of Appeals for the Second Circuit in the *Doe* v. *Mukasey* decision.

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." S. 1692 as reported expands oversight by mandating new audits by the Department of Justice, Office of Inspector General, requiring new court-approved minimization procedures on surveillance authorities, and including more detailed public reporting on the use of surveillance under FISA.

II. History of the Bill and Committee Consideration

A. Introduction of the Bill

The USA PATRIOT Act Sunset Extension Act of 2009 was introduced as S. 1692 on September 22, 2009 by Senators Leahy, Cardin, and Kaufman. Senator Sanders joined as a cosponsor on September 25, 2009. Prior to the first executive business meeting at which the bill was debated, Senator Leahy developed a substitute amendment with Senator Feinstein. The substitute was laid down as the pending amendment in an executive business meeting on October 1, 2009. The substitute amendment was cosponsored by Senators Leahy, Feinstein, Cardin, Kaufman, Sanders, Whitehouse, and Klobuchar.

B. Committee Consideration

1. Hearing

The Committee held a hearing titled, "Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security," on September 23, 2009. During the first panel, testimony was received 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 are presently set to expire on December 31, 2009, are the roving wiretap authority, the "lone wolf" surveillance authority, and the provision authorizing orders for business records and other tangible things. Mr. Kris stated that the Department would be pleased to work with Congress as it considered other changes to law, but presently was not able to take a position on S. 1692. Mr. Kris' testimony reflected a letter sent by Ronald Weich, Assistant Attorney General for Legislative Affairs, to Chairman Leahy on September 14, 2009, which is available upon request.

Mr. Fine's testimony 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 USA PATRIOT Improvement and Reauthorization Act of 2005 (Pub. L. No. 109–177).

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. Written testimony is available at *http://judiciary.senate.gov/hearings/hearing.cfm?id=4062.*

Additional material was submitted by the Vermont Library Association, the American Association of Law Libraries, the Constitution Project, and the American Civil Liberties Union.

2. Executive business meetings

The bill was placed on the Committee's agenda for consideration on September 24, 2009. It was held over on that date.

On October 1, 2009, the Committee on the Judiciary considered S. 1692 during an executive business meeting. Chairman Leahy offered a manager's amendment, in the nature of a complete substitute, which was adopted by unanimous consent and subject to amendment. The substitute was cosponsored by Senators Leahy, Feinstein, Cardin, Kaufman, Sanders, Whitehouse, and Klobuchar.

The substitute amendment made a number of clarifying changes and other modifications to S. 1692 as introduced. First, the sunset on NSLs was modified such that rather than fully expiring on December 31, 2013, the NSL authority would revert to the standards in law prior to the enactment of the 2001 PATRIOT Act. The substitute strikes the renewable one-year time limit on nondisclosure orders for NSLs to allow a recipient of a nondisclosure order to challenge it in court at any time. Under the substitute amendment, the court may set the terms of nondisclosure as appropriate. The substitute ensures that the FBI will prepare a written statement of facts showing relevancy to an authorized investigation before an NSL can be issued. It also clarifies that the statement will be retained by the FBI, and not issued to the NSL recipient. It will be available for internal review and audits by the Inspector General.

The substitute amendment struck the three-part standard for pen trap and trace orders, and for section 215 orders, except in the case of library records.

The substitute amendment was adopted by unanimous consent. Senators Feingold, Durbin and Specter each requested that they be recorded as voting "no."

Senator Durbin offered an amendment to strike the standard in S. 1692 for issuing a section 215 order for business records and other tangible things and replace it with a three-part standard. The amendment was rejected by a roll call vote.

The vote record is as follows:

Tally: 4 Yeas, 15 Nays

Yeas (4): Feingold (D–WI), Durbin (D–IL), Cardin (D–MD), Specter (D–PA).

Nays (15): Kohl (D–WI), Feinstein (D–CA), Schumer (D–NY), Whitehouse (D–RI), Klobuchar (D–MN), Kaufman (D–DE), Franken (D–MN), Sessions (R–AL), Hatch (R–UT), Grassley (R–IA), Kyl (R–AZ), Graham (R–SC), Cornyn (R–TX), Coburn (R–OK), Leahy (D–VT).

Senator Feingold offered an amendment to S. 1692 to modify the presumptive time period for delayed notice search warrant from 30 days, which is the period under current law, to seven days. The amendment was accepted by a roll call vote.

The vote record is as follows:

Tally: 12 Yeas, 7 Nays

Yeas (12): Kohl (D–WI), Feinstein (D–CA), Feingold (D–WI), Schumer (D–NY), Durbin (D–IL), Cardin (D–MD), Whitehouse (D–RI), Klobuchar (D–MN), Kaufman (D–DE), Specter (D–PA), Franken (D–MN), Leahy (D–VT).

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

Senators Kyl and Schumer offered an amendment which would have amended the criminal identity theft provisions in title 18 of the United States Code to make it a Federal crime to produce or use a false travel document. The amendment was withdrawn by Senator Kyl.

Senator Sessions offered a motion to strike the sunset provision for NSLs from S. 1692. This motion was rejected by a roll call vote.

The vote record is as follows:

Tally: 6 Yeas, 13 Nays

Yeas (6): Sessions (R–AL), Hatch (R–UT), Grassley (R–IA), Kyl (R–AZ), Graham (R–SC), Cornyn (R–TX).

Nays (13): Kohl (D–WI), Feinstein (D–CA), Feingold (D–WI), Schumer (D–NY), Durbin (D–IL), Cardin (D–MD), Whitehouse (D–RI), Klobuchar (D–MN), Kaufman (D–DE), Specter (D–PA), Franken (D–MN), Coburn (R–OK), Leahy (D–VT).

Senator Kyl offered an amendment which would have amended the Classified Information Protection Act (CIPA) in a variety of ways, including authorizing interlocutory appeals for any order for access to classified information, allowing CIPA requests to be made *ex parte*, and limiting the ability of the court to decide when defense counsel may review classified evidence. The amendment was withdrawn by Senator Kyl.

On October 8, 2009, the Committee on the Judiciary resumed consideration of S. 1692.

Senator Sessions offered a package of amendments to S. 1692 that would make technical fixes and add clarifying language to address concerns about the effectiveness and efficiency of certain provisions. The amendments are as follows:

Senator Sessions offered an amendment to clarify that minimization procedures for pen register and trap and trace orders apply to information "known to concern" U.S. persons. This modification clarifies that investigators are expected to apply the required minimization protections based on their knowledge at the time about the subject of an investigation.

Senator Sessions offered an amendment to provide that if the conditions set forth for a nondisclosure order on NSLs are met, judges shall issue the order.

Senator Sessions offered an amendment to limit the Government's duty to notify NSL recipients when nondisclosure orders are no longer required to those instances where a recipient has previously challenged the order.

Senator Sessions offered a perfecting amendment that makes the description of library records consistent with the language used in current law under subsection (a) of Section 215 and clarifies when library records are entitled to more deferential review.

Senator Sessions offered an amendment that makes technical fixes to minimization procedures for pen register and trap and trace orders to clarify the intent of this provision.

The package of amendments offered by Senator Sessions was adopted by voice vote.

Senator Durbin offered an amendment to require a three-part standard for issuing NSLs. The amendment failed by a roll call vote.

The vote record is as follows:

Tally: 4 Yeas, 15 Nays

Yeas (4): Feingold (D–WI), Durbin (D–IL), Cardin (D–MD), Specter (D–PA).

Nays (15): Kohl (D–WI), Feinstein (D–CA), Schumer (D–NY), Whitehouse (D–RI), Klobuchar (D–MN), Kaufman (D–DE), Franken (D–MN), Sessions (R–AL), Hatch (R–UT), Grassley (R–IA), Kyl (R–AZ), Graham (R–SC), Cornyn (R–TX), Coburn (R–OK), Leahy (D–VT).

Senator Kyl offered an amendment to strike the standard of "appropriate weight" that the court must give to the Government's request for a nondisclosure order for NSLs and instead require the court to afford the Government's request for such a nondisclosure order "substantial weight." This amendment was adopted by a voice vote.

Senator Feingold offered an amendment to require the Attorney General to issue minimization procedures for the use of NSLs within 180 days of the enactment of the bill. The amendment was agreed to by voice vote.

Senator Kyl offered an amendment to strike "specific and articulable facts" from the written statement that the FBI or other agency issuing an NSL must prepare to show that the information it is requesting is relevant to its investigation. The amendment was modified to only strike "and articulable" from the statement of facts. The amendment as modified was agreed to by a roll call vote.

The vote record is as follows:

Tally: 14 Yeas, 4 Nays, 1 Pass

Yeas (14): Kohl (D–WI), Feinstein (D–CA), Schumer (D–NY), Whitehouse (D–RI), Klobuchar (D–MN), Kaufman (D–DE), Franken (D–MN), Sessions (R–AL), Grassley (R–IA), Kyl (R–AZ), Graham (R–SC), Cornyn (R–TX), Coburn (R–OK), Leahy (D–VT) .

Nays (4): Feingold (D–WI), Durbin (D–IL), Cardin (D–MD), Hatch (R–UT).

Pass (1): Specter (D–PA).

Senator Feingold offered an amendment to prevent the Government from using the warrantless collection authorities of the FISA Amendments Act to conduct "bulk collection." Senator Feingold withdrew the amendment.

Senator Feingold offered an amendment to allow the "lone wolf" provision to expire on December 31, 2009. This amendment failed on a roll call vote.

The vote record is as follows:

Tally: 3 Yeas, 16 Nays

Yeas (3): Feingold (D–WI), Durbin (D–IL), Specter (D–PA).

Nays (16): Kohl (D–WI), Feinstein (D–CA), Schumer (D–NY), Cardin (D–MD), Whitehouse (D–RI), Klobuchar (D–MN), Kaufman (D–DE), Franken (D–MN), Sessions (R–AL), Hatch (R–UT), Grassley (R–IA), Kyl (R–AZ), Graham (R–SC), Cornyn (R–TX), Coburn (R–OK), Leahy (D–VT).

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, 8 Nays

Yeas (11): Kohl (D–WI), Feinstein (D–CA), Schumer (D–NY), Cardin (D–MD), Whitehouse (D–RI), Klobuchar (D–MN), Kaufman (D–DE), Franken (D–MN), Kyl (R–AZ), Cornyn (R–TX), Leahy (D–VT).

Nays (8): Feingold (D–WI), Durbin (D–IL), Specter (D–PA), Sessions (R–AL), Hatch (R-UT), Grassley (R–IA), Graham (R–SC), 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 2009."

Section 2. Sunsets

This section extends the sunsets on the provisions for "lone wolf," roving wiretaps and orders for tangible things from December 31, 2009 to December 31, 2013. This section establishes a sunset of December 31, 2013, on the use of NSLs. 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.

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 circulation records or patron lists, the Government must meet a higher standard. That standard is 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.

This section also requires court review of minimization procedures.

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 provision 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.

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 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 re-

peals 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*, 07–4943–cv (December 15, 2008), and adopts the concepts suggested by that court for a constitutionally sound process. Id. at pp. 39–40. 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. The Government must notify any entity that challenges a nondisclosure order when the need for nondisclosure is terminated.

The bill requires FISA court approval of minimization procedures, 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 statement of specific facts showing 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.

Section 8. Public reporting on National Security Letters

This section requires annual public reporting on the number of requests for NSLs. and greater specificity of the types of persons targeted (e.g., U.S. persons v. non-U.S. persons).

Section 9. Public reporting on the Foreign Intelligence Surveillance Act

This section requires annual public reporting of aggregate numbers of requests for surveillance that also includes a breakdown of requests for (a) electronic surveillance, (b) physical searches, (c) orders for tangible things (section 215 orders), and (d) pen registers. Current law requires only public reporting of the above categories in the aggregate.

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.

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. In reducing the initial period of delayed notice from 30 to 7 days, the Committee does not intend to suggest that it would be improper for courts to continue to grant extensions of up to 90 days, where appropriate, as they do at present.

Section 12. NSL minimization procedures

Current law does not require minimization procedures be established, but the Department was required by law to conduct a feasibility study on the matter. The Office of Inspector General's audits on NSLs, which found past misuse and abuse of the NSL authority, called for minimization procedures to be established. This section requires that the Attorney General, within 180 days of enactment, establish minimization and destruction procedures governing acquisition, retention, and dissemination by the FBI of any records received by the FBI in response to an NSL.

IV. Congressional Budget Office Cost Estimate

The Committee sets forth, with respect to the bill, S. 1692, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

October 23, 2009.

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. 1692, the USA PATRIOT Act Sunset Extension Act of 2009.

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. 1692—USA PATRIOT Act Sunset Extension Act of 2009

CBO estimates that implementing S. 1692 would cost about $5 million over the 2010–2012 period and less than $500,000 annually in subsequent years, assuming the availability of appropriated

funds. Enacting the bill could affect direct spending and revenues, but CBO estimates that any such effects would not be significant.

CBO has determined that the provisions of S. 1692 are either excluded from review for mandates under the Unfunded Mandates Reform Act because they are necessary for national security or contain no intergovernmental or private-sector mandates.

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. 1692 would extend for four years certain provisions of those acts that will otherwise expire on December 31, 2009. In addition, the bill would modify the laws relating to certain investigations of potential terrorist activity and require the Department of Justice (DOJ) to prepare additional reports and audits relating to those investigations.

S. 1692 would require the DOJ Inspector General, by December 31, 2012, to conduct audits of the department's use of certain investigative powers during the 2007–2011 period. Based on information from DOJ, we expect that the department would need to hire about 10 people to carry out the audits. CBO estimates that it would cost about $1 million in fiscal year 2010, about $2 million annually over the 2011–2012 period, and less than $500,000 annually thereafter for DOJ to complete the audits and reports required by the bill. Such spending would be subject to the availability of appropriated funds.

Because those prosecuted and convicted under S. 1692 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.

The CBO staff contact for this estimate is Mark Grabowicz. The estimate was approved by Peter H. Fontaine, 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. 1692, as reported, the Department of Justice would be required to issue minimization procedures on NSLs, section 215 orders, and pen register and trap and trace devices.

VI. Conclusion

The USA PATRIOT Act Sunset Extension Act of 2009, S. 1692, 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 con-

stitutional 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 December 31, 2009, the Committee recommends swift action on S. 1692 as reported.

VII. Additional and Minority Views

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

On September 23, 2009, the Senate Judiciary Committee held a hearing entitled, "Reauthorizing the USA PATRIOT Act: Ensuring Liberty and Security," at which David Kris, the Assistant Attorney General for the National Security Division, testified about the importance of the authorities contained in the USA PATRIOT Improvement and Reauthorization Act of 2005. Underscoring Mr. Kris's testimony, the Department of Justice indicted terror suspect Najibullah Zazi just one day after the Committee's hearing[1] for his role in what Attorney General Eric Holder has called "one of the most serious terrorist threats to our country since September 11, 2001."[2]

According to the official Department of Justice press release accompanying the indictment, Mr. Zazi "knowingly and intentionally conspired with others to use one or more weapons of mass destruction, specifically explosive devices, against persons or property within the United States."[3] The *New York Times* described the government's case against Mr. Zazi as "a set of damning accusations" that begin "with explosives training in Pakistan, followed by purchases of bomb-making materials in Colorado, experiments in a hotel room, and a cross-country trip to New York, which the authorities feared might have been the target of the attack."[4] The facts surrounding this terrorist plot become even more alarming in light of reports that Mr. Zazi was in contact with senior al Qaeda operatives, including Mustafa Abu al-Yazid, the leader of al Qaeda in Afghanistan.[5]

As the Zazi case makes clear, the terrorist threat is not abating. If anything, today's terrorist organizations are more sophisticated, more determined and more aware of our efforts to combat their tactics than ever before. As President Obama said earlier this month in his October 20 address to the New York Joint Terrorism Task Force: "We all know that we are facing a determined adversary. . . . They are resourceful, they are resilient, they are still plotting, as we have become all too aware." Now is not the time to risk

---

[1] Press Release, Office of Public Affairs, Department of Justice, Najibullah Zazi Indicted for Conspiracy (Sept. 24, 2009), *available at http://www.justice.gov/opa/pr/2009/September/09-ag-1017.html* (hereinafter "Press Release").

[2] "Holder: NYC Terror Plot Most Serious Since 9/11," Newsday, Oct. 6, 2009, *available at http://www.newsday.com/news/new-york/holder-nyc-terror-plot-most-serious-since-9-11-1.1505916*.

[3] Press Release, *supra* n. 1.

[4] David Johnston and William K. Rashbaum, "Rush for Clues Before Charges in Terror Case," N.Y. Times, Oct. 1, 2009.

[5] "Zazi Linked to Al Qaeda's Afghan Head," CBS News, Oct. 14, 2009, *available at http://www/cbsnews.com/stories/2009/10/14/national/main5384355.shtml*.

weakening the legal authorities that our national security professionals rely upon every day to detect and prevent attacks.

PATRIOT Act and FISA authorities have been vital to our counterterrorism efforts in recent years. For example, PATRIOT Act tools appear to have contributed to last month's arrest of Mr. Zazi.[6] PATRIOT Act authorities also reportedly played a role in thwarting the terrorist plot uncovered earlier this year in New York, in which four former convicts who converted to radical Islam plotted to use explosives to blow up synagogues and shoot down an airplane with a surface-to-air missile at an Air National Guard base.[7]

These are not new developments. Over the last eight years, law enforcement officials have given the PATRIOT Act credit for cracking major terrorism cases and preventing attacks throughout the country, including in California, New York, Texas, Ohio, and Virginia.

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. Although these legal tools were most recently renewed as part of the PATRIOT Act reauthorization in 2005 and 2006, three critical important provisions of the PATRIOT Act will, without further legislative action, no longer be available after December 31, 2009. These provisions are:

- **The "roving wiretap" provision, Section 206 of the USA PATRIOT Act.** This tool allows investigators to follow sophisticated terrorists who are trained to evade detection (for example, by rapidly changing cell phone numbers). This authority protects agents from having to file repetitious court applications to continue an investigation every time a terrorist changes phones. 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 business records in national security terrorism cases. Examining business records often provides key information that assists investigators in solving a wide range of crimes.
- **The "lone wolf" authority, Section 6001 of the Intelligence Reform and Terrorism Prevention Act**. This authority allows intelligence investigations of terrorists who are not connected to a foreign nation or 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 20th hijacker in the 9/11 attacks), when agents did not get a search warrant

[6] "Notice of Intent To Use Foreign Intelligence Surveillance Act Information," *United States v. Najibullah Zazi*, U.S. District Court for the District of Colorado, Docket No. 09–cr–03001–CBS, September 21, 2009.

[7] Cristina Corbin, "Patriot Act Likely Helped Thwart NYC Terror Plot, Security Experts Say," FOX News, May 21, 2009, *available at http://www.foxnews.com/politics/2009/05/21/ security-experts-say-patriot-act-likely-helped-thwart-nyc-terror-plot/*.

for his computer because they believed that they could not show that he was an agent of a foreign power.

A broad bipartisan group of 89 Senators—including then-Senators Obama and Biden—supported these tools when they voted in favor of the PATRIOT Act reauthorization legislation in 2006. The Department of Justice strongly supports the renewal of all three of these measures. In addition to writing to Senator Leahy in detail regarding why each of these authorities is critical, both David Kris,[8] the Assistant Attorney General for the National Security Division, and FBI Director Robert Mueller[9] have testified before the Judiciary Committee in support of renewing the expiring authorities.

All three of these tools have helped protect the nation from terrorist threats and provide our investigators and analysts with critical information. In order to continue to protect the nation, this Committee's highest priority should be to renew these tools. All other issues and controversies should be put aside and considered as part of other legislation. As some of us have stated previously, we prefer a simple, four-year renewal of these three authorities. There is no need to tie other matters, such as changes to the use of national security letters ("NSLs"), to renewal of these important provisions.

We appreciate and are encouraged by this Committee's bipartisan commitment in S. 1692 to reauthorize these three authorities until 2013. Due in large part to amendments several of us offered during the Committee's consideration of this measure, we are also encouraged that the Committee-approved version of S. 1692 was considerably improved over the previous versions circulated. Unfortunately, we remain concerned that portions of this bill will substantially weaken the Government's ability to protect the nation against terrorism and other national security threats.

OUR AMENDMENTS TO IMPROVE S. 1692

As part of the Committee's consideration of S. 1692, Senators Sessions and Kyl offered, and the Committee accepted, seven amendments to address deficiencies in the legislation.

First, the Committee adopted an amendment offered by Senator Sessions that makes clear that a restriction on the distribution of non-public information obtained from pen registers only applies to information known to concern U.S. persons. Before this amendment was adopted, S. 1692 provided that minimization procedures would "prohibit the dissemination of non-publicly available information concerning unconsenting United States persons." This language was problematic from an operational perspective, as investigators frequently do not know at an early stage of an investigation whether the telephone numbers they are looking at belong to U.S. persons or others. The prior language would have required agents to take a closer look at each number dialed to determine whether or not that number belongs to a U.S. person, simply to comply with

[8] *See* "Statement of David Kris," before the Committee on the Judiciary, United States Senate, Sept. 23, 2009, *available at http://judiciary.senate.gov/pdf/09-09-23%20Kris%20Testimony.pdf*.

[9] Carie Johnson, "FBI Chief Urges Renewal of Patriot Act," Washington Post, Mar. 26, 2009, *available at http://www.washingtonpost.com/wp-dyn/content/article/2009/03/25/AR2009032501862.html* (calling provisions "exceptional tools to promote national security").

the procedures. This would have introduced a new privacy concern where one did not previously exist. This amendment makes clear that the prohibition only applies to those unconsenting U.S. persons that are known.

Second, Senator Sessions offered an amendment adopted by the Committee to require courts to issue a NSL nondisclosure order if the government meets the required burden. Before this amendment was adopted, if the government met the statutory burden, the bill stated only that "the court *may* issue a nondisclosure order . . . ." (emphasis added). In other words, even if the government established that disclosure would result in "a danger to the national security of the United States," a court could still refuse to enforce the nondisclosure requirement. This was problematic from an operational perspective. Judges should not have the unfettered discretion to refuse to issue nondisclosure orders once the government has met its burden. If the government has shown that nondisclosure is needed, the order should issue.

Third, the Committee adopted an amendment offered by Senator Sessions that clarifies whom the government must notify regarding the termination of an NSL nondisclosure requirement. Previously, the bill required the FBI to monitor when "the facts supporting a nondisclosure requirement cease to exist" and notify the recipient that "the nondisclosure requirement is no longer in effect." This requirement would have been an operational impossibility for the FBI, as it issues thousands of NSLs every year. Requiring the FBI to look back on both active and cold investigations to keep tabs in every case on when nondisclosure is no longer warranted will be a logistical nightmare and could lead to compliance problems. This amendment altered this requirement by making notification necessary only to those entities that had already notified the government that they wished to have a court review the nondisclosure requirement.

Fourth, Senator Sessions offered an amendment adopted by the Committee that changes the types of records that qualify for the new and heightened "library records" provisions contained in S. 1692. Under the previous language, this higher standard applied if the records sought "pertain[] to" libraries. This language was problematic. A court could interpret the "pertains to" language very broadly, making the job of national security investigators much more difficult. For example, a telephone company complying with a Section 215 order might believe it has to spend countless hours combing through phone records to see if they include the number of a library. Similarly, banks might have to do the same to see if bank records contain credit card payments for library fines. This amendment applies the heightened library standard only where "the records sought are the circulation records or patron lists of a library." It is our understanding that this language is supported by the Administration.

Fifth, the Committee adopted another amendment offered by Senator Sessions to address the new minimization requirements for pen registers. Under current law, there are no minimization requirements for either criminal law or FISA pen registers. This is logical, since pen registers by definition do not capture content. Instead, they simply gather raw telephone data (for example, a list

of numbers) that are building blocks of an investigation. Before this amendment was adopted, S. 1692 imposed minimization requirements on pen registers. These requirements would have led to considerable operational confusion, as both the FISA Court and agents would have struggled to apply minimization procedures, designed to protect U.S. person information, to data that is not readily identifiable as being U.S. person information. It makes sense to instead limit these minimization requirements to those cases where judges feel privacy interests are particularly at play. This amendment removes the mandate that minimization take place in the pen register context and instead gives courts the discretion to impose minimization requirements in exceptional circumstances. It is our understanding that this language is supported by the Administration.

Sixth, Senator Kyl offered an amendment adopted by the Committee that addresses that standard of deference a court will give to a determination by national security officials that the disclosure of an NSL would present a danger to national security. Under existing law, such a certification is given "conclusive" effect, absent a showing of bad faith by the certifying official. In *Doe* v. *Mukasey*,[10] the U.S. Court of Appeals for the Second Circuit held that this standard was too deferential, as "some demonstration from the Executive Branch of the need for secrecy is required in order to conform the nondisclosure requirement to First Amendment standards." However, S. 1692 went way beyond what *Doe* requires, as it would give the certification of national security danger only "appropriate weight." This language was problematic for a variety of reasons, including the fact that "appropriate weight" is a standard alien to national security jurisprudence, and is seemingly malleable to the whims of the particular federal judge handling any one case. This amendment substitutes an oft-used, familiar standard by requiring a court to give "substantial weight" to a government certification that the disclosure of an NSL would present a danger to national security. It is our understanding that this language is supported by the Administration.

Seventh, the Committee adopted an amendment offered by Senator Kyl that addresses a provision of the bill that requires the FBI to maintain a "written statement" for every NSL issued. As the bill was drafted, the statement would need to contain "specific and articulable facts" that justify the need for the NSL. Although this sounds like mere recordkeeping, the "specific and articulable facts" language could have caused operational problems. Currently, NSLs are available for use in what are defined as "preliminary investigations" under FBI Guidelines. The problem is that the "specific and articulable facts" language resembles the standard the FBI Guidelines require for a later, more-developed stage in an investigation, i.e., what it deems a "full investigation." This language was amended to make clear that NSLs are still available at the "preliminary investigation" stage of a national security investigation by the FBI. This amendment, as orally amended in markup, kept the requirement for the "written statement" and also kept the substitute bill's requirement that such a statement have a basis in "specific facts." However, this amendment drops the words "and articulable" in

[10] 549 F.3d 861, 882 (2nd Cir. 2008).

order to avoid giving the impression that Congress was changing the FBI's owns standards for when NSLs can be used.

SPECIFIC DEFICIENCIES IN S. 1692

Although these and other amendments improve S. 1692, we continue to have reservations regarding this bill. In particular, we are concerned that by placing a four-year sunset and new and burdensome minimization requirements on NSLs, as well as unnecessary burdens on business record requests and delayed notice search warrants, this legislation will make it more difficult for investigators and analysts to obtain the information they need to make the necessary decisions to protect the country. Although we have concerns with other parts of this legislation, we will focus on these particular deficiencies.

Imposing new "minimization" procedures on NSLs

Section 12 of S. 1692 requires the Attorney General to issue minimization procedures for NSLs within 180 days of enactment of this legislation. At the time the Committee adopted this provision via amendment, Members believed the minimization procedures were already being considered and implemented within the Department of Justice. As the amendment sponsor stated during the markup prior to the Committee's vote: "What I said was I know of nobody saying we should not do this. They are working on it. We are telling them to get it done in a timely manner."[11] In recent days, however, administration officials from the Department of Justice and Federal Bureau of Investigations advised Committee staff that the procedures the Department is currently drafting for NSLs differ significantly from the minimization procedures required by Section 12. Accordingly, the Committee's adoption of Section 12 appears to be based on a misunderstanding.

Current law already imposes significant burdens on the government in its efforts to obtain records pursuant to NSLs in national security and terrorism cases. As noted previously, NSLs give national security agencies some of the powers dozens of domestic agencies already possess in areas far less critical than national security. Indeed, a 2002 study conducted by the Department of Justice Office of Legal Policy "identified approximately 335 administrative subpoena authorities existing in current law," including for agencies ranging from the Appalachian Regional Commission to the Commodities Future Trading Commission and Environmental Protection Agency.[12]

NSLs are already more difficult to obtain than normal subpoenas. Unlike administrative subpoenas, NSLs have to be approved by a senior FBI official. Several layers of oversight are also built into the system to prevent abuse. For example, NSL use is

[11] *See* Transcript of Executive Business Meeting at 71, Committee on the Judiciary, United States Senate, Oct. 8, 2009, *available at http://www.senate.gov/fplayers/CommPlayer/commFlashPlayer.cfm?fn=judiciary100809&st=xxx* (min. 117:56 to 118:03).

[12] U.S. Department of Justice Office of Legal Policy, Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities, May 2002, *available at http://www.justice.gov/archive/olp/rpt_to_congress.htm. See also* Testimony of Rachel Brand, Principal Deputy Assistant Attorney General, Office of Legal Policy, before the United States Senate Judiciary Committee, Subcommittee on Terrorism, Technology and Homeland Security, June 22, 2004.

monitored and reviewed by the FBI's Office of General Counsel, and by the National Security Law Branch of the Justice Department. This assures that there is scrutiny of field office use and headquarters oversight of the use of NSLs. In addition, the type of information that can be obtained with an NSL is limited by law to specific areas, such as telephone subscriber information or employment location.

Minimization requirements should not be applied to early-stage investigative tools such as NSLs because these types of process generally do not result in the collection of the contents of communications. Further, investigators often do not know whether the information they have obtained is even relevant to their investigation. For example, if an agent obtained a list of phone numbers, that agent would have no idea whether the obtained numbers belonged to U.S. persons or others. Minimization could require investigators to take a closer look at each number obtained to determine whether or not that number belonged to a U.S. person, simply to comply with the procedures. This would introduce a new privacy concern where one did not previously exist.

Although minimization requirements were imposed on Section 215 orders in 2005, the Department of Justice only issued thirteen requests for such orders as recently as 2008.[13] By contrast, many more NSLs concerning U.S. persons were issued last year.[14] We have learned in recent days that the imposition of minimization procedures on this broadly used and important national security tool would have a devastating impact on national security investigations, contrary to the understanding of Members at the markup of S. 1692.[15] Current reporting requirements, along with zealous Inspector General oversight, are sufficient to ensure that NSLs are being used appropriately. Requiring the Justice Department to formulate and issue NSL minimization procedures within 180 days will cause serious operational difficulties for national security investigators, particularly in light of all the questions that will be raised as to the implementation of the procedures.

Dramatic Shortening of Period for Delayed Notice Search Warrants

We are also concerned about Section 3 of S. 1692, which would considerably shorten the notification period for delayed notice search warrants from thirty days to a mere seven days—less than a quarter of the time allowed under current law. Reducing the time period for delay of search warrant notification arbitrarily places disclosure risks into the most secret actions a government can engage. The new disclosure requirements, if adopted, will force investigators to return to the issuing judge less than a week after they first received the warrant. Investigators should be spending their

[13] *See* "FISA Report to Congress: 2008," U.S. Dept. of Justice, Office of Legislative Affairs, May 14, 2009, at *4 *available at http://www.fas.org/irp/agency/doj/fisa/2008rept.pdf*.

[14] *See id*.

[15] *See* Transcript of Executive Business Meeting at 70–71, Committee on the Judiciary, United States Senate, Oct. 8, 2009, *available at http://www.senate.gov/fplayers/CommPlayer/commFlashPlayer.cfm?fn=judiciary100809&st=xxx* (min. 117:12 to 117:29) (Sen. Russ Feingold states, "I do not know of anybody over there that is saying we should not do this. They are working on it. They think we ought to do it. The FBI thinks we ought to do it. The Attorney General thinks you ought to do it. They just have not gotten it done. We are just telling them to get it done. So the notion that somehow this is some terrible idea flies in the face of the very people you are often quoting as saying this.").

time bringing offenders to justice, not at the courthouse deluging courts with unnecessary paperwork.

We are concerned that debate during the Committee's markup centered on two cases to the exclusion of other case law on this issue. In fact, the two cases cited in support of this provision predate the original PATRIOT Act by more than a decade. In *United States* v. *Freitas*,[16] the U.S. Court of Appeals for the Ninth Circuit set as a standard that notice must be given within "a reasonable, but short, time" and ruled that that period could not exceed seven days absent "a strong showing of necessity." Four years later, the Second Circuit reached a similar conclusion but articulated a different standard. In *United States* v. *Villegas*,[17] the court held that delay is permissible if investigators show there is "good reason" for the delay. The U.S. Court of Appeals for the Second Circuit agreed with the Ninth Circuit that the initial delay should not exceed seven days but allowed for further delays if each is justified by "a fresh showing of the need for further delay."

We believe these two cases are outliers. In other jurisdictions, courts imposed longer delay periods, if time limits were set at all.[18] The whole point of section 213 of the PATRIOT Act (as refined in 2006) was to create a middle-ground, nationwide standard for delayed notice search warrants. There is simply no basis to go back to the time limit that existed in a handful of courts prior to the enactment of the PATRIOT Act. Furthermore, there is no need to change the law to abridge the time allowed for delayed notification. No federal court has overturned a post-PATRIOT Act search on the ground that the delayed notice standard in section 213 (codified at 18 U.S.C. 3103a(b)(3)) is unconstitutional under the Fourth Amendment.

Sunset on National Security Letters

Section 2 of S. 1692 places a new and unnecessary four-year sunset on the PATRIOT Act amendments made to the national security letter statutes. According to Section 2 of S. 1692, on December 31, 2013, NSLs may only be issued pursuant to the considerably more rigorous standard that existed before the enactment of the PATRIOT Act. As a practical matter, this sunset will virtually eliminate the use of NSLs.

NSLs are a valuable tool and have provided investigators and analysts with critical information.[19] 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 opera-

[16] 800 F.2d 1451 (9th Cir. 1986).

[17] 899 F.2d 1324 (2d Cir. 1990).

[18] *See, e.g.*, *United States* v. *Simons*, 206 F.3d 392 (4th Cir. 2000) (45-day delay constitutional); *United States* v. *Hernandez*, 07–60027–CR, 2007 WL 2915856 (S.D. Fla. Oct. 4, 2007) (unpublished) (noting there is no similar time limit [to that in *Villegas*] suggested or required in [the 11th] Circuit.").

[19] *See e.g.* "FBI Press Conference on DOJ Inspector General's Report of Use of National Security Letters," FBI, March 9, 2007, *available at http://www.fbi.gov/pressrel/pressrel07/nsl_transcript030907.htm* (stating "national security letters are a critical tool and are the bread and butter of our investigations.").

tives."[20] 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."[21] 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."[22]

Section 2 of S. 1692 rescinds these valuable tools by, starting in 2013, requiring the government to follow the cumbersome pre-PATRIOT Act NSL standard. Prior to the PATRIOT Act, not only did the requested records have to be relevant to an investigation, but the FBI also had to have specific and articulable facts giving reason to believe that the information requested pertained to a foreign power or an agent of a foreign power, such as a terrorist or spy. This pre-PATRIOT Act requirement kept the FBI from using NSLs to develop evidence at the early stages of an investigation, which is precisely when they are the most useful, and often prevented investigators from acquiring records that were relevant to an ongoing international terrorism or espionage investigation.

In 2005, Matthew Berry, Counselor to the Assistant Attorney General for the Office of Legal Policy, provided this example of the problems caused by the old standard:

> Let's say that post-2001 and this has happened—you capture a terrorist, and on the terrorist's computer you have a series of phone numbers. Any investigator worth his or her salt would want to take those phone numbers and figure out the subscriber information, whose phone numbers they are, and in many cases toll billing records, . . . what numbers have been calling that phone number and what numbers has that phone number been calling. . . . Prior to the PATRIOT Act we couldn't use NSLs to obtain that information because we had no idea whatsoever whose phone numbers they were. They could be a terrorist associate's phone numbers. They could be the drycleaner's phone numbers. We needed the basic information to forward the investigation. We couldn't use it for that purpose."[23]

Mr. Berry further explained the benefit of the PATRIOT Act amendments to the NSL statutes: "Now, because the standard is

---

[20] *See* "Statement of Matthew Berry," Counselor to the Assistant Attorney General, Office of Legal Policy, U.S. Dept. of Justice, before the House Subcommittee on Crime, Terrorism, and Homeland Security, May 26, 2005, at *5, *available at http://www.usdoj.gov/olp/pdf/usa_patriot_act_reauthorization_matthew_berry_testimony.pdf.*

[21] *See* "A Review of the Federal Bureau of Investigation's Use of National Security Letters," U.S. Dept. of Justice, Office of Inspector General, March 2007, at xxii, *available at http://www.usdoj.gov/oig/special/s0703b/final.pdf.*

[22] *See* "Statement of Valerie Caproni Before the House Committee on the Judiciary," March 20, 2007, *available at http://www.fbi.gov/congress/congress07/caproni032007.htm.*

[23] Testimony of Matthew Berry (Oral), Counselor to the Assistant Attorney General, Office of Legal Policy, U.S. Department of Justice, before the House Subcommittee on Crime, Terrorism, and Homeland Security, May 26, 2005.

relevance, the same standard that we have in criminal investigations with grand jury subpoenas, we can obtain that information. And I can report . . . that such uses of the NSLs have been very valuable to the Department and have allowed us to identify terrorist operatives that we previously did not know about. So I think that it would be a major, major mistake to return back to the prior standard."[24]

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 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 standard 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 Department of Justice has responded to these improper practices and is taking action to ensure that they are not repeated. For example, the use of so-called "exigent letters" has been forbidden. 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."[25] What is puzzling is that the supposed remedy in S. 1692—a sunset of the NSL standard to what it was before September 11, 2001—generally has no relationship whatsoever to the deficiencies related to NSLs found by the Inspector General.

Business and library records

Although we are pleased with some of the modifications adopted by the Committee to Section 3 of S. 1692 to remedy potential operational concerns, we remain concerned that Section 3 continues to place too high a burden on the government's ability to obtain business records. Current law already imposes significant burdens on the efforts of investigators to obtain business records in national security and terrorism cases. For example, under current law, the government must submit a statement of facts showing reasonable grounds to believe that the business records sought are relevant to an authorized investigation. Under the current system, records are presumptively relevant if the government meets certain requirements. Unfortunately, S. 1692 removes that presumption and instead requires investigators to tell the court the reasons why the records are relevant. It is not necessary to make investigators

[24] *Id.*

[25] *See* "A Review of the Federal Bureau of Investigation's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006," U.S. Dept. of Justice, Office of Inspector General, March 2008, at 15, *available at http://www.usdoj.gov/oig/special/s0803b/final.pdf.*

spend their time doing this when they are dealing with agents of foreign powers, as opposed to uninvolved U.S. persons.

Additionally, Section 3 provides unnecessary and curious protections for library records. If a library is involved, S. 1692 requires the government to prove to the court that the business records sought pertain to a foreign power or an agent of a foreign power. If investigators cannot make this showing, they cannot use the records, even if they could otherwise satisfy a court that there were reasonable grounds to believe that the business records sought were relevant to an authorized investigation.

S. 1692 suggests that national security investigators have some sort of curious interest in the library habits of ordinary Americans. There is simply no evidence to support this allegation. We do know, however, that terrorists and spies have used libraries to plan and carry out activities that threaten our national security. In 2005, then-Deputy Attorney James Comey told the House Judiciary Committee about the dangers in treating libraries differently from any other entity:

> Prosecutors have always been able to obtain records from libraries and bookstores through grand jury subpoenas. Libraries and booksellers should not become safe havens for terrorists and spies. Last year, a member of a terrorist group closely affiliated with al Qaeda used Internet service provided by a public library to communicate with his confederates. Furthermore, we know that spies have used public library computers to do research to further their espionage and to communicate with their co-conspirators. For example, Brian Regan, a former TRW employee working at the National Reconnaissance Office, who was convicted of espionage, extensively used computers at five public libraries in Northern Virginia and Maryland to access addresses for the embassies of certain foreign governments.[26]

As Mr. Comey explained, we simply should not allow libraries to become safe havens for terrorist or clandestine activities.

ADDITIONAL ISSUES

In addition to the previously discussed problems, it is our understanding that there are several other issues and problems the Administration would like addressed in this legislation. We concur with the following particular criticisms and suggestions:

- An effective date for the statute should be added to give the government sufficient time to make necessary adjustments to systems and processes to accommodate the new law.
- With respect to the public reporting requirements of S. 1692, both the NSL and FISA reporting requirements should be altered to ensure that no publicly disclosed information could be used by enemies of the United States to thwart surveillance or to discern classified aspects of intelligence programs.

[26] Testimony of James Comey, Deputy Attorney General, before the House Committee on the Judiciary (June 8, 2005).

- Section 3(a)(3)(B)(iii) of S. 1692 provides that orders under Section 501(c) of FISA should include the requirement that the order "shall direct that the minimization procedures be followed." This should be corrected by a technical amendment to Section 501.
- A provision should be added to ensure that current orders issued pursuant to the statute will remain in effect until they would be due for renewal.
- It should be made clear that the changes to the business record and pen register statutes are intended to codify current practice under the relevance standard and are not intended to prohibit or restrict any activities approved by the FISA Court under existing authorities.
- It should be made clear that the new provision regarding minimization in exceptional cases is intended merely to codify the court-imposed minimization regime with respect to certain programs, and is not intended to require minimization in other contexts.

CONCLUSION

Although we support the Committee's efforts to reauthorize the three expiring PATRIOT Act provisions, we are deeply concerned by some of the changes in S. 1692 that could create unforeseen difficulties in ongoing and future counterterrorism investigations. We are especially concerned by language adopted in the Committee that would severely complicate the use of NSLs.

The threat of violent Islamist extremism remains, not only from al-Qaeda but now also from al-Qaeda allied terrorist organizations operating around the world and lone wolf terrorists operating on their own here in the United States. The Zazi case and others make it clear that this is no time to let our guard down. Just weeks before U.S. officials identified Zazi as a possible terrorist threat, John Brennan, President Obama's Assistant for Homeland Security and Counterterrorism, stated publicly that "another attack on the U.S. homeland remains the top priority for the al Qaeda senior leadership."

Our intelligence and law enforcement professionals need a complete and immediate reauthorization of the expiring PATRIOT Act authorities in order to continue their efforts to combat the terrorist threat at home and abroad. As recent arrests and indictments demonstrate, these vital tools are being used responsibly and wisely by law enforcement 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 hope S. 1692 can be modified before final passage to create a more narrow reauthorization bill that creates fewer questions about the impact on operations.

JEFF SESSIONS.
ORRIN G. HATCH.
CHUCK GRASSLEY.
JON KYL.
LINDSEY GRAHAM.

JOHN CORNYN.
TOM COBURN.

ADDITIONAL VIEWS FROM SENATOR KYL AND SENATOR CORNYN

We have numerous concerns with this bill, most of which are explained in the statement of additional views that we signed with Senators Sessions, Hatch, Grassley, Graham, and Coburn. Simply put, this bill would make many changes to current law that we believe are unwarranted and unwise given the continuing threat of terrorism, the demonstrated effectiveness of the PATRIOT Act tools in combating this threat,[1] and the civil liberties safeguards that are already part of the PATRIOT Act.[2] We write separately to explain why, notwithstanding our broad concerns about the overall policy direction being taken in this bill, we supported reporting it from the Committee.

The bill that was originally before the Committee had a number of provisions that would have directly affected ongoing and future national security investigations in an adverse way. The Chairman's substitute amendment was a step in the right direction—it addressed some of those operational impacts. But in a classified setting, officials from the Department of Justice, the Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence confirmed that several provisions in the substitute bill still could cause significant operational problems.

Senator Sessions offered a number of amendments to address specific concerns identified in that classified briefing. These amendments were accepted. In addition, Senator Kyl offered two amendments. The first required that a court give "substantial weight" to a government certification that the disclosure of the issuance of a national security letter would present a danger to national security. Prior to adoption of this amendment, the bill required only that a court give such a certification "appropriate weight." The second amendment offered by Senator Kyl clarified that the bill's new requirement that the FBI prepare and maintain a "written statement" for every national security letter issued would not be misconstrued as discouraging the use of national security letters for preliminary investigations. It did this by requiring that a written

[1] For instance, PATRIOT Act tools appear to have played an important role in the arrest of terror suspect Najibullah Zazi. *See* "Notice of Intent To Use Foreign Intelligence Surveillance Act Information," *United States* v. *Najibullah Zazi*, U.S. District Court for the District of Colorado, Docket No. 09–cr–03001–CBS, September 21, 2009; Christina Corbin, "Patriot Act Likely Helped Thwart NYC Terror Plot, Security Experts Say," FOX News, May 21, 2009, *available at http://www.foxnews.com/politics/2009/05/21/security-experts-say-patriot-act-likely-helped-thwart-nyc-terror-plot/*.

[2] One example of the protections afforded by the PATRIOT Act is the ability of a party to challenge a Section 215 business records order. On September 14, 2009, the Department of Justice sent a letter to Chairman Leahy that said: "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."

statement be based on "specific"—as opposed to "specific and articulable"—facts. As with the amendments offered by Senator Sessions, the adoption of these amendments reduced the potential operational effects of the bill.

Even with these improvements, the bill might still create operational problems. For example, an amendment to require the FBI to establish "minimization procedures" for national security letters was agreed to over the objection of many members, including ourselves. The amendment was described as having the support of the Administration and as requiring only that the Department of Justice and the FBI finalize procedures that are already close to completion.[3] After the Committee voted to report the bill, however, the Justice Department and the FBI expressed serious objections to the amendment. According to them, the national security procedures that are being drafted might not be viewed by a court as "minimization procedures," as would be required by the amendment. Moreover, the Department of Justice and the FBI expressed doubt that FISA-type "minimization procedures" were feasible in the national security letters context. In fact, they feared that "minimization procedures" would pose substantial and undesirable obstacles to the use of this important tool. The Department of Justice and the FBI also raised a number of other issues that they believe must be addressed before the bill can be considered operationally neutral, including changes to the bill's public reporting and audit provisions and the inclusion of effective date language.

In light of the critical need to reauthorize the expiring provisions by the end of the year, the progress that has been made to improve the bill thus far, and, most importantly, our understanding that the bill's sponsors will continue to work in good faith with us to address any remaining adverse operational impacts that the bill might have, we voted to keep this bill moving forward. We did this despite serious misgivings about the policy direction that the bill takes in many areas (for example, the imposition of a new sunset

---

[3] *See* Transcript of Executive Business Meeting at 68–72, Committee on the Judiciary, United States Senate, Oct. 8, 2009, *available at http://www.senate.gov/fplayers/CommPlayer/commFlashPlayer.cfm?fn=judiciary100809&st=xxx* (min. 114:04–118:20). In relevant part, the transcript reads:

Senator Feingold. So people are clear before we vote. This amendment is not about the standard for issuing NSLs. That was the previous amendment that Senator Durbin and I offered. It is about requiring the Executive Branch itself to have its own internal procedures, which the IG specified were inadequate and we do not specify what they will be.

* * *

Senator Feingold. Just very quickly, I want to reiterate what the Chairman just said. I do not know of anybody over there that is saying we should not do this. They are working on it. They think we ought to do it. The FBI thinks we ought to do it. The Attorney General thinks you ought to do it. They just have not gotten it done. We are just telling them to get it done. So the notion that somehow this is some terrible idea flies in the face of the very people you are often quoting as saying this.

Senator Kyl. Senator Feingold, would you allow me to just interrupt you for a comment then? If this amendment is adopted and if it turns out that the statement you just made is correct, then I will back off my opposition. If it turns out that the statement is incorrect, I would hope we could revisit this. In other words, if the FBI says this is going to potentially impede our operations with respect to these kinds of letters—your statement was that they say that they are okay, that we need them.

Senator Feingold. What I said was I know of nobody saying we should not do this. They are working on it. We are telling them to get it done in a timely manner. So, sure, if you find somebody——

Senator Kyl. If you would be willing to——

Senator Feingold. But nobody is saying that and they are working on it.

Senator Leahy. Do you want a voice vote or roll call?

Senator Kyl. Mr. Chairman, at this time, I will just register my objection based upon the agreement Senator Feingold and I have and then I do not require a roll call vote.

on national security letters). It is our hope that, with the help of the Department of Justice and the FBI, we can continue to identify and fix provisions of the bill that could have an adverse operational effect. We will be able to support the final product only if it does not impede the government's ability to investigate and prevent terrorist activities. In this regard, the interaction of the House and Senate will be critical.

JON KYL.
JOHN CORNYN.

MINORITY VIEWS FROM SENATORS FEINGOLD, DURBIN AND SPECTER

S. 1692, as reported by this Committee, contains improvements over current law that we support. Nonetheless, we voted against reporting the bill because we believe it does not go far enough. We commend the Chairman for his efforts to include new civil liberties protections in this bill, including important transparency and oversight measures. Our concerns are generally not with what is in the bill; they are with what is missing: adequate protections for the privacy of innocent Americans. The government needs strong tools to combat terrorism, but those tools also need to be subject to sufficient safeguards and robust oversight.

There can be no doubt that significant statutory changes are needed. In 2007, the Department of Justice Inspector General concluded in a lengthy report that there had been "widespread and serious misuse of the FBI's national security letter authorities. In many instances, the FBI's misuse of national security letters violated NSL statutes, Attorney General Guidelines, or the FBI's own internal policies." The USA PATRIOT Act vastly expanded the National Security Letter (NSL) statutes, and the government can issue NSLs without judicial review. The 2007 Inspector General report stated that 22% of NSL requests were not reported in the FBI tracking database. It further identified more than 700 instances in which the FBI improperly obtained telephone toll billing records through the use of "exigent letters." A recent FBI briefing conveyed that after an internal review, the FBI identified 4,379 unique numbers that were contained in either exigent letters or so-called "Blanket NSLs" (which were issued in an attempt to provide legal process for information previously obtained via exigent letters or oral requests). Of those, 610 were purged because the FBI could not reconcile the data with any appropriate legal process. The Inspector General also documented that the use of NSLs has been increasing, particularly to gather information on U.S. persons. According to the 2008 Inspector General report, the percentage of NSL requests generated from investigations of U.S. persons grew from 39% in 2003 to 57% in 2006. During this same time frame, NSL requests relating to non-U.S. persons remained relatively stable, while the number of requests relating to U.S. persons grew from 6,519 in 2003 to 11,517 in 2006.

We appreciate the steps that the FBI has taken to address the problems identified by the Inspector General's reports, but ultimately we believe statutory reforms are needed to ensure that such problems do not recur. And this is just one example; the USA PATRIOT Act dramatically expanded other surveillance authorities that also are not yet subject to adequate statutory protections.

We preferred the original version of S. 1692 that the Chairman introduced over the Committee-reported version. The substitute

amendment weakened some of the most substantial privacy protections that were in the original version of the bill.

Nonetheless, the bill does contain some important improvements. We support the new Department of Justice Inspector General audit requirements. It is due to similar provisions that the Chairman championed in the 2005 reauthorization legislation that we now know about the extensive misuse of the National Security Letter authorities by the FBI. The public reporting requirements in S. 1692 will help bring additional transparency to how National Security Letters and Foreign Intelligence Surveillance Act authorities are used. And changes to the provisions governing NSL and Section 215 nondisclosure orders help bring those provisions in line with the First Amendment.

We strongly support the inclusion of a change to the statute governing delayed notification criminal search warrants, 18 U.S.C. § 3103a, which was enacted as part of the USA PATRIOT Act and permits the government to secretly search people's houses in the course of ordinary criminal investigations and not notify them until weeks or months later. The Committee-reported bill shortens the presumptive time period for delayed notice from 30 days to 7 days. A July 2009 report of the Administrative Office of the U.S. Courts confirmed that these so-called "sneak and peek" warrants are only very rarely used in terrorism cases. Given the very substantial privacy interests at stake, we are pleased that the bill shortens the presumptive notification period.

The bill also contains new four-year sunsets, including for the first time a sunset for National Security Letters. It would be our preference to finally fix these authorities once and for all, but it is important to note that establishing sunsets will require Congress to reconsider these authorities in the future. We do question the need to extend the so-called "lone wolf" authority, given that it has never been used and that it raises serious constitutional questions.

We also agree with the provision in the bill requiring that minimization procedures for Section 215 orders be court-approved. We were disappointed that a similar provision for FISA pen register and trap and trace device orders was modified during the markup process to essentially make pen/trap minimization procedures optional. We were pleased that the Committee adopted by voice vote an amendment offered by Senator Feingold that would require the Attorney General within 180 days to issue minimization procedures for National Security Letters. This was a recommendation of the Department of Justice Inspector General, who testified as follows at the September 23, 2009, Senate Judiciary Committee hearing:

> We believe that the Department should promptly . . . issue final minimization procedures for NSLs that address the collection of information through NSLs, how the FBI can upload NSL information in FBI databases, the dissemination of NSL information, the appropriate tagging and tracking of NSL derived information in FBI databases and files, and the time period for retention of NSL obtained information. At this point, more than 2 years have elapsed since after our first report was issued, and final guidance is needed and overdue.

We agree with the Inspector General that these procedures need to be completed. We understand that the FBI and Justice Department have been working on this, and we believe that a statutory mandate to promulgate such procedures in combination with a firm deadline will ensure this recommendation is implemented. Of course, procedures governing the acquisition, retention and dissemination of records obtained via National Security Letters will be different from minimization procedures established for the collection of the full contents of communications. It nonetheless remains important that such procedures be established, particularly because National Security Letters are used without any FISA Court review or oversight.

New sunsets, audits, reporting requirements and executive branch procedures are positive reforms, but ultimately Congress must set the rules for when the Executive Branch can use investigative tools that have implications for Americans' privacy rights. That is why we were disappointed that the Committee rejected amendments that would have imposed stricter statutory standards for obtaining any tangible things under Section 215 of the USA PATRIOT Act and for obtaining sensitive personal records under the NSL statutes—standards that would have protected against government fishing expeditions.

The standard under current law for both authorities is mere relevance to an investigation to protect against international terrorism or clandestine intelligence activities. That is a very broad standard, which does not provide, in our view, adequate protection against unnecessary, overbroad, or otherwise inappropriate demands for records. Senator Durbin offered amendments that would have changed the standard—for both Section 215 and NSLs—to require some connection, however remote, to a suspected terrorist or spy. Specifically, the standard he proposed would require the government to demonstrate that the records sought are relevant to a national security investigation, *and* that the records (1) pertain to an agent of a foreign power; (2) pertain to someone in contact with or known to an agent of a foreign power; *or* (3) are relevant to the activities of an agent of a foreign power.

This is the same standard that the Committee-reported bill would impose on the use of Section 215 to obtain library circulation records and patron lists. While library records are particularly sensitive, so are other records that can be obtained with Section 215 orders, such as medical and bookseller records. Thus, we believe this standard should apply to all records and other tangible things sought under Section 215, not just library records. Indeed, the original version of S. 1692 did just that, but that important protection was limited to library records in the complete substitute. The three-part standard that Senator Durbin proposed would give the FBI the authority and flexibility it needs to conduct intelligence investigations, while also ensuring that the records it collects have some direct or indirect connection to a suspected terrorist or spy—an important protection for innocent Americans.

It is also important to note that this three-part standard is not a new proposal. When the Committee considered USA PATRIOT Act reauthorization legislation in 2005, it unanimously reported a bill, S. 1389 (109th Cong.), that contained this standard for Section

215 orders. That bill then passed the Senate by unanimous consent in July 2005. We believe this provision should be included in this reauthorization legislation for Section 215 orders, NSLs, and FISA pen/traps—and that the failure to do so is the biggest gap in the legislation.

We also would have preferred that the Committee-reported bill include additional modifications to address, among other things, the permanent, automatic gag orders that are imposed on all recipients of Section 215 orders; the language in FISA that permits the government to obtain so-called "John Doe" roving wiretap orders based simply on a "description" of a target; and the circumstances in which criminal sneak and peek search warrants are allowed. Many of the reforms we support are included in S. 1686, the JUSTICE Act, which Senator Feingold introduced.

In sum, we believe Congress should take the opportunity presented by this reauthorization process to reform the surveillance authorities so dramatically expanded by the USA PATRIOT Act once and for all. S. 1692 contains additional transparency measures, sunsets that will force Congress to revisit these issues in four years, and some important but modest changes to the authorities that raise civil liberties concerns. However, we believe additional checks and balances are needed and therefore we opposed reporting the bill in this form to the full Senate.

RUSSELL D. FEINGOLD.
RICHARD DURBIN.
ARLEN SPECTER.

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. 1692, 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 [FN1] 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 of-

fice, 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 appropriate 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 agency 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).

(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.

* * * * * * *

TITLE 18—CRIMES AND CRIMINAL PROCEDURE

PART I—CRIMES

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, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, no wire or electronic communications service provider, or officer, employee, or agent thereof, shall disclose to

any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request) that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

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

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

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

(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 the 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 subsection (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 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 and articulable 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 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 re-

view 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 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 device, 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*, and if, in exceptional circumstances, minimization procedures are ordered, that 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 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 are the circulation records or patron lists of a library (as defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1))), 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. [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 accord-

ance 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 Director 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 Gov-

ernment 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.

* * * * * * *

Subchapter V—Reporting Requirement

SEC. 1871. 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) PUBLIC REPORT.—The Attorney General shall make publicly available the portion of each report under subsection (a) relating to paragraphs (1) and (2) of subsection (a).

(c)[(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.

(d)[(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).

(e)[(d)] PROTECTION OF NATIONAL SECURITY.—The Attorney General, in consultation with the Director of National Intelligence, may authorize redactions of materials described in *subsection* (d) [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.

(f)[(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.

* * * * * * *

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 December 31, [2009] *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;

(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

(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 *each of calendar years 2006 through 2011* [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;

(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 June 30, 2011, 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 December 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 2010 and 2011.

(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), *(c)(2), (c)(3), or (c)(4)* [or (c)(2)], the Inspector General of the Department of Justice 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), *(c)(2), (c)(3), or (c)(4)* [and (c)(2)] as the Attorney General or the Director of National Intelligence may consider necessary.

(e) UNCLASSIFIED FORM.—The reports submitted under subsections (c)(1), *(c)(2), (c)(3), or (c)(4)* [and (c)(2)] and any comments included under subsection (d)(2) shall be in unclassified form, but may include a classified annex.

* * * * * * *

SEC. 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) CONTENT.—

(A) IN GENERAL.—Except as provided in subparagraph (B), each report required under this subsection shall include the total number of requests described in paragraph (1) requiring disclosure of information concerning—

(i) United States persons;

(ii) persons who are not United States persons;

(iii) persons who are the subjects of authorized national security investigations; or

(iv) persons who are not the subjects of authorized national security investigations.

(B) EXCEPTION.—With respect to the number of requests for subscriber information under section 2709 of title 18, United States Code, a report required under this subsection need not provide information separated into each of the categories described in subparagraph (A).

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

* * * * * * *

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 Se-

lect 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 June 30, 2011, 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 December 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 2010 and 2011.

(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), *(c)(2), (c)(3), or (c)(4)* **[**or (c)(2)**]**, the Inspector General of the Department of Justice 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), *(c)(2), (c)(3), or (c)(4)* **[**or (c)(2)**]** as the Attorney General or the Director of National Intelligence may consider necessary.

(e) UNCLASSIFIED FORM.—The reports submitted under subsection (c)(1), *(c)(2), (c)(3), or (c)(4)* **[**or (c)(2)**]** and any comments included under subsection (d)(2) shall be in unclassified form, but may include a classified annex.

(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 proce-

dures 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).

* * * * * * *

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.

* * * * * * *

New Provisions Under USA PATRIOT Act Sunset Extension Act of 2009 (S. 1692)

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 section 624 of such Act read on October 25, 2001;

(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 or any other department or agency of the Federal Government;

(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 (as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801));

(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 (as 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

(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 June 30, 2011, 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 December 21, 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 2010 and 2011.

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

(A) NOTICE.—Not less than 30 days before the submission of a report under subparagraph (A) or (B) of paragraph (3), the Inspector General of the Department of Justice 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 a report submitted under subparagraph (A) or (B) of paragraph (3) as the Attorney General or the Director of National Intelligence may consider necessary.

(5) UNCLASSIFIED FORM.—A report submitted under subparagraph (A) or (B) of paragraph (3) and any comments included under paragraph (4)(B) shall be in unclassified form, but may include a classified annex.

* * * * * * *

SEC. 12. MINIMIZATION.

(a) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Attorney General shall—

(1) establish minimization procedures governing the acquisition, retention, and dissemination by the Federal Bureau of Investigation of any records received by the Federal Bureau of Investigation in response to a national security letter; and

(2) 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 Intel-

ligence of the House of Representatives a copy of the minimization procedures established under paragraph (1).

(b) DEFINITIONS.—In this section—

(1) the term "minimization procedures" means—

(A) specific procedures that are reasonably designed in light of the purpose and technique of a national security letter, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons (as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)) 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 101(e)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(e)(1))) shall not be disseminated in a manner that identifies any United States person, without the consent of the United States person, unless the identity of the United States person 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; and

(2) the term "national security letter" means 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)), subsection (a) or (b) of 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).

○