111TH CONGRESS } HOUSE OF REPRESENTATIVES { REPT. 111–382
1st Session } { Part 1

USA PATRIOT AMENDMENTS ACT OF 2009

DECEMBER 16, 2009.—Ordered to be printed

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

R E P O R T

together with

DISSENTING VIEWS

[To accompany H.R. 3845]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 3845) to extend and modify authorities needed to combat terrorism and protect civil liberties, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

89–006

THE AMENDMENT

The amendment is as follows:
Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "USA PATRIOT Amendments Act of 2009".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

TITLE I—USA PATRIOT ACT RELATED AMENDMENTS

SEC. 101. ROVING WIRETAPS.

Section 105(c)(2)(B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(c)(2)(B)) is amended by striking "finds, based upon specific facts" and inserting "finds—

"(i) that the target of the application is a foreign power, as defined in paragraph (1), (2), (3), or (6) of section 101(a), an agent of such a foreign power, or a specific individual; and

"(ii) based upon specific facts".

SEC. 102. EXTENSION OF SUNSET OF SECTIONS 206 AND 215 OF USA PATRIOT ACT.

Section 102(b)(1) of the USA PATRIOT Improvement and Reauthorization Act of 2005 (18 U.S.C. 2510 note) is amended by striking "December 31, 2009" and inserting "December 31, 2013".

SEC. 103. ACCESS TO CERTAIN TANGIBLE THINGS UNDER SECTION 501 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

(a) FACTUAL BASIS FOR AND ISSUANCE OF ORDERS.—

(1) IN GENERAL.—Section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861) is amended—

(A) in the section heading, by striking "**CERTAIN BUSINESS RECORDS**" and inserting "**TANGIBLE THINGS**"; and

(B) in subsection (b)(2)(A)—

(i) by striking "a statement of facts showing" and inserting "a statement of the facts and circumstances relied upon by the applicant to justify the belief of the applicant"; and

(ii) by striking "clandestine intelligence activities" and all that follows and inserting "clandestine intelligence activities;".

(2) TECHNICAL AND CONFORMING AMENDMENTS.—

(A) TITLE HEADING.—Title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) is amended in the title heading by striking "CERTAIN BUSINESS RECORDS" and inserting "TANGIBLE THINGS".

(B) TABLE OF CONTENTS.—The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is amended by striking the items relating to title V and section 501 and inserting the following:

"TITLE V—ACCESS TO TANGIBLE THINGS FOR FOREIGN INTELLIGENCE PURPOSES

"Sec. 501. Access to tangible things for foreign intelligence and international terrorism investigations.".

(b) JUDICIAL REVIEW OF FISA ORDERS.—Section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861) is amended—

(1) in subsection (c)(2)—

(A) in subparagraph (D) by striking "things; and" and inserting "things;";

(B) in subparagraph (E), by striking "subsection (a)." and inserting "subsection (a); and"; and

(C) by adding at the end the following new subparagraph:

"(F) shall direct the applicant to provide notice to each person receiving such order of—

"(i) the right to challenge the legality of a production order or nondisclosure order by filing a petition in accordance with subsection (f); and

"(ii) the procedures to follow to file such petition in accordance with such subsection."; and

(2) in subsection (f)(2)—

(A) in subparagraph (A)—

(i) in clause (i)—

(I) by striking "a production order" and inserting "a production order or nondisclosure order"; and

(II) by striking "Not less than 1 year" and all that follows;

(ii) in clause (ii), by striking "production order or nondisclosure"; and

(B) in subparagraph (C)—

(i) by striking clause (ii); and

(ii) by redesignating clause (iii) as clause (ii).

(c) MINIMIZATION PROCEDURES.—Section 501(g) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861(g)) is amended—

(1) by redesignating paragraph (2) as paragraph (3); and

(2) by inserting after paragraph (1) the following new paragraph:

"(2) COMPLIANCE ASSESSMENT.—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 such order, a judge may assess compliance with the minimization procedures required to be followed under such order by reviewing the circumstances under which information concerning United States persons was retained or disseminated.".

(d) REQUIREMENTS FOR ORDERS FOR CERTAIN RECORDS FROM LIBRARIES.—Section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861) is amended—

(1) in subsection (b)(2)—

(A) by redesignating subparagraph (B) as subparagraph (C); and

(B) by inserting after subparagraph (A) the following new subparagraph:

"(B) if the records sought contain bookseller information, or are from a library (as defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1))) and contain personally identifiable information about a patron of such library, a statement of specific and articulable 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 who is the subject of such authorized investigation; and"; and

(2) by adding at the end the following new subsection:

"(i) BOOKSELLER INFORMATION DEFINED.—In this section, the term 'bookseller information' means personally identifiable information concerning the purchase (including subscription purchases) or rental of books, journals, or magazines, whether in print or digitally.".

SEC. 104. SUNSET RELATING TO INDIVIDUAL TERRORISTS AS AGENTS OF FOREIGN POWERS.

Section 6001(b) of the Intelligence Reform and Terrorism Prevention Act of 2004 (50 U.S.C. 1801 note; Public Law 108–458) is amended—

(1) in paragraph (1)—

(A) by striking "the amendment made by subsection (a) shall cease to have effect" and inserting "effective"; and

(B) by striking the period and inserting "—

"(A) subparagraph (C) of section 101(b)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(b)(1)) is repealed;

"(B) subparagraphs (D) and (E) of such section are redesignated as subparagraphs (C) and (D), respectively;

"(C) paragraph (2) of section 601(a) of such Act (50 U.S.C. 1871(a)) is repealed; and

"(D) paragraphs (3), (4), and (5) of such section are redesignated as paragraphs (2), (3), and (4), respectively."; and

(2) in paragraph (2)—

(A) by striking "EXCEPTION.—With respect to" and inserting "EXCEPTION.—

"(A) EXISTING INVESTIGATIONS.—With respect to"; and

(B) by adding at the end the following new subparagraph:

"(B) REPORTS.—Notwithstanding the repeals made by paragraph (1), the first report required under section 601(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871(a)) that is submitted after the effective date of such repeals shall include the number of individuals covered by an order issued pursuant to section 101(b)(1)(C) of such Act (as in effect on the day before such effective date).".

SEC. 105. AUDITS.

(a) TANGIBLE THINGS.—Section 106A of the USA PATRIOT Improvement and Reauthorization Act of 2005 (Public Law 109–177; 120 Stat. 200) is amended—

(1) in subsection (b)—

(A) in paragraph (1), by striking "2006" and inserting "2013"; and

(B) in paragraph (5)(C), by striking "calendar year 2006" and inserting "each of calendar years 2006 through 2013";

(2) in subsection (c), by adding at the end the following:

"(3) CALENDAR YEARS 2007 THROUGH 2009.—Not later than December 31, 2010, 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 through 2009.

"(4) CALENDAR YEARS 2010 THROUGH 2013.—Not later than December 31, 2011, and annually thereafter until December 31, 2014, 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 the preceding calendar year.";

(3) in subsection (d)—

(A) in paragraph (1), by striking "or (c)(2)" and inserting ", (c)(2), (c)(3), or (c)(4)"; and

(B) in paragraph (2), by striking "and (c)(2)" and inserting ", (c)(2), (c)(3), or (c)(4)"; and

(4) in subsection (e), by striking "and (c)(2)" and inserting ", (c)(2), (c)(3), or (c)(4)".

(b) NATIONAL SECURITY LETTERS.—Section 119 of the USA PATRIOT Improvement and Reauthorization Act of 2005 (Public Law 109–177; 120 Stat. 219) is amended—

(1) in subsection (b)(1), by striking "2006" and inserting "2013";

(2) in subsection (c), by adding at the end the following:

"(3) CALENDAR YEARS 2007 THROUGH 2009.—Not later than December 31, 2010, 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 through 2009.

"(4) CALENDAR YEARS 2010 THROUGH 2013.—Not later than December 31, 2011, and annually thereafter until December 31, 2014, 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 the previous calendar year.";

(3) in subsection (d)—

(A) in paragraph (1), by striking "or (c)(2)" and inserting ", (c)(2), (c)(3), or (c)(4)"; and

(B) in paragraph (2), by striking "or (c)(2)" and inserting ", (c)(2), (c)(3), or (c)(4)"; and

(4) in subsection (e), by striking "or (c)(2)" and inserting ", (c)(2), (c)(3), or (c)(4)".

(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 by the Federal Government, 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.) and section 3122 of title 18, United States Code, during the period beginning on January 1, 2007 and ending on December 31, 2012.

(2) REQUIREMENTS.—The audits required under paragraph (1) shall include—

(A) an examination of each instance in which the Attorney General or any other attorney for the Government submitted an application for an order or extension of an order under title IV of the Foreign Intelligence Surveillance Act of 1978, including whether the court granted, modified, or denied the application (including an examination of the basis for any modification or denial);

(B) an examination of each instance in which the Attorney General authorized the installation and use of a pen register or trap and trace device on an emergency basis under section 403 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1843);

(C) whether the Federal Bureau of Investigation requested that the Department of Justice submit an application for an order or extension of an order under title IV of the Foreign Intelligence Surveillance Act of 1978 and the request was not submitted to the court (including an examination of the basis for not submitting the application);

(D) whether bureaucratic or procedural impediments to the use of pen registers and trap and trace devices under title IV of the Foreign Intelligence Surveillance Act of 1978 prevent the Federal Bureau of Investigation from taking full advantage of the authorities provided under that title;

(E) 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

(F) 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 through 2012, an examination of the minimization procedures used in relation to pen registers and trap and trace devices under title IV of the Foreign Intelligence Surveillance Act of 1978 and whether the minimization procedures protect the constitutional rights of United States persons;

(iv) whether, and how often, the Federal Bureau of Investigation used information acquired under a pen register or trap and trace device under title IV of the Foreign Intelligence Surveillance Act of 1978 to produce an analytical intelligence product for distribution within the

Federal Bureau of Investigation, to the intelligence community (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 December 31, 2010, 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 thorough 2009.

(B) CALENDAR YEARS 2010 THROUGH 2013.—Not later than December 31, 2011, and annually thereafter until December 31, 2014, 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 the previous calendar year.

(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. 106. CRIMINAL "SNEAK AND PEEK" SEARCHES.

Section 3103a of title 18, United States Code, is amended—

(1) in subsection (b)—

(A) in paragraph (1), by striking "may have an adverse result (as defined in section 2705, except if the adverse results consist only of unduly delaying a trial)" and inserting "may endanger the life or physical safety of an individual, result in flight from prosecution, result in the destruction of or tampering with the evidence sought under the warrant, or result in intimidation of potential witnesses, or is likely to otherwise seriously jeopardize an investigation or unduly delay a trial"; and

(B) in paragraph (3), by striking "30 days" and all that follows and inserting "7 days after the date of its execution."; and

(2) in subsection (c), by striking "for good cause shown" and all that follows and inserting "upon application of the United States Attorney for the district seeking the delay, for additional periods of not more than 21 days for each application, if the court finds, for each application, reasonable cause to believe that notice of the execution of the warrant may endanger the life or physical safety of an individual, result in flight from prosecution, result in the destruction of or tampering with the evidence sought under the warrant, or result in intimidation of potential witnesses, or is likely to otherwise seriously jeopardize an investigation or unduly delay a trial.".

SEC. 107. ORDERS FOR PEN REGISTERS AND TRAP AND TRACE DEVICES FOR FOREIGN INTELLIGENCE PURPOSES.

(a) APPLICATION.—Section 402(c) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1842(c)) is amended—

(1) in paragraph (1), by striking "and" at the end;

(2) in paragraph (2)—

(A) by striking "a certification by the applicant" and inserting "a statement of the facts relied upon by the applicant to justify the belief of the applicant"; and

(B) by striking the period at the end and inserting "; and"; and

(3) by adding at the end the following:

"(3) a statement of proposed minimization procedures.".

(b) MINIMIZATION.—

(1) DEFINITION.—Section 401 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1841) is amended by adding at the end the following:

"(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.".

(2) PEN REGISTERS AND TRAP AND TRACE DEVICES.—Section 402 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1842) is amended—

(A) in subsection (d)(2)—

(i) in subparagraph (C)(i)(VII), by striking "; and" and inserting ";";

(ii) in subparagraph (C)(ii)(IV), by striking the period at the end and inserting "; and"; and

(iii) by adding at the end the following new subparagraph:

"(D) shall, if the judge finds that there are exceptional circumstances, direct that minimization procedures be followed."; and

(B) by adding at the end the following:

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

(3) EMERGENCIES.—Section 403 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1843) is amended—

(A) by redesignating subsection (c) as subsection (d); and

(B) by inserting after subsection (b) the following:

"(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.".

(4) USE OF INFORMATION.—Section 405(a)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1845(a)(1)) is amended by inserting "and the minimization procedures under this title, if required" after "provisions of this section".

SEC. 108. PUBLIC REPORTING ON THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

Section 601 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871) is amended—

(1) by redesignating subsections (b) through (e) as subsections (c) through (f), respectively;

(2) by inserting after subsection (a) the following:

"(b) PUBLIC REPORT.—The Attorney General shall make publicly available the portion of each report under subsection (a) relating to paragraph (1) of such subsection."; and

(3) in subsection (e), as so redesignated, by striking "subsection (c)" and inserting "subsection (d)".

SEC. 109. CHALLENGES TO NATIONWIDE ORDERS FOR ELECTRONIC EVIDENCE.

Section 2703 of title 18, United States Code, is amended by adding at the end the following:

"(h) JUDICIAL REVIEW.—A provider of electronic communication service or remote computing service may challenge a subpoena, order, or warrant requiring disclosure of customer communications or records under this section in—

"(1) the United States district court for the district in which the order was issued; or

"(2) the United States district court for the district in which the order was served.".

SEC. 110. REPORT ON CIVIL LIBERTIES AND PRIVACY PROTECTIONS.

Not later than 180 days after the date of the enactment of this Act, the President 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 describing—

(1) whether operations conducted pursuant to orders issued under section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861) could be modified in a manner that enhances protections for civil liberties; and

(2) the nature of any potential modifications, the likely costs of such modifications, any technical challenges, and any potential impact on such operations.

TITLE II—NATIONAL SECURITY LETTER REFORM

SEC. 201. SHORT TITLE.

This title may be referred to as the "National Security Letter Reform Act of 2009".

SEC. 202. SUNSET.

(a) IN GENERAL.—Effective on December 31, 2013, the following provisions of law are amended to read as such provisions read on October 25, 2001:

(1) Section 2709 of title 18, United States Code.

(2) Section 1114(a)(5) of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3414(a)(5)).

(3) Subsections (a) and (b) of section 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u).

(4) Section 627 of the Fair Credit Reporting Act (15 U.S.C. 1681v).

(5) Section 802 of the National Security Act of 1947 (50 U.S.C. 436).

(b) TRANSITION PROVISION.—Notwithstanding subsection (a), the provisions of law referred to in subsection (a), as in effect on December 30, 2013, shall continue to apply 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.

SEC. 203. NATIONAL SECURITY LETTER DEFINED.

In this title, 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 626 of the Fair Credit Reporting Act (15 U.S.C. 1681u) (to obtain certain financial information and consumer reports).

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

(5) Section 802 of the National Security Act of 1947 (50 U.S.C. 436).

SEC. 204. MODIFICATION OF STANDARD.

(a) IN GENERAL.—A national security letter may not be issued unless the official having authority under law to issue that letter documents in a separate writing specific and articulable facts showing that there are reasonable grounds to believe that the information sought—

(1) pertains to a foreign power or an agent of a foreign power;

(2) is relevant to the activities of a suspected agent of a foreign power that is the subject of such authorized investigation; or

(3) pertains to an individual in contact with, or personally known to, a suspected agent of a foreign power that is the subject of such authorized investigation.

(b) MAINTENANCE.—The agency under whose authority a national security letter is issued shall maintain a copy of a separate writing required under subsection (a).

(c) DEFINITIONS.—In this section, the terms "foreign power" and "agent of a foreign power" have the meaning given such terms in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

SEC. 205. NOTIFICATION OF RIGHT TO JUDICIAL REVIEW OF NONDISCLOSURE ORDER.

If a recipient of a national security letter is subject to a nondisclosure requirement imposed in connection with that national security letter, the official issuing that letter shall, simultaneously with its issuance, inform the recipient of the right

of the recipient to judicial review of that requirement and that the requirement will remain in effect during the pendency of any judicial review proceedings.

SEC. 206. DISCLOSURE FOR LAW ENFORCEMENT PURPOSES.

No information acquired by a national security letter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information may only be used in a criminal proceeding with the advance authorization of the Attorney General, or a designee of the Attorney General at a level not lower than Section Chief of a division of the Department of Justice.

SEC. 207. JUDICIAL REVIEW OF NATIONAL SECURITY LETTER NONDISCLOSURE ORDER.

Section 3511(b) of title 18, United States Code, is amended to read as follows:

"(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 (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, 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 particular information about 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 may issue a nondisclosure order for a period of not longer than 180 days.

"(D) DENIAL.—If a district court of the United States rejects an application for a nondisclosure order or extension thereof, the nondisclosure requirement shall no longer be in effect.

"(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, of the existence of a result described in subparagraphs (A) through (D) and 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 may issue a nondisclosure requirement order or extension thereof under this subsection if the court determines that there is reason to believe that disclosure of the information subject to the nondisclosure requirement during the applicable time period will have a result described in paragraph (2).

"(4) RENEWAL.—A nondisclosure order under this subsection may be renewed for additional periods of not longer than 180 days each, upon a determination by the court that a result described in paragraph (2) justifies the renewal.

"(5) EARLY TERMINATION OF NONDISCLOSURE ORDER.—A nondisclosure order the Government applied for under paragraph (1)(B) ceases to have effect when the Government discovers that the factual basis for that order has ceased to exist and the Government so informs the order's recipient. The Government upon making such a discovery shall promptly so informs the recipient.".

SEC. 208. 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 Intelligence 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 request for information 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).

SEC. 209. PUBLIC REPORTING ON NATIONAL SECURITY LETTERS.

Section 118(c) of the USA PATRIOT Improvement and Reauthorization Act of 2005 (18 U.S.C. 3511 note) is amended—

(1) in paragraph (1)—

(A) in the matter preceding subparagraph (A), by striking "concerning different United States persons"; and

(B) in subparagraph (A), by striking ", excluding the number of requests for subscriber information";

(2) by redesignating paragraph (2) as paragraph (3); and

(3) by inserting after paragraph (1) the following:

"(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).".

TITLE III—GENERAL PROVISIONS

SEC. 301. SENSE OF CONGRESS ON LEVEL OF CLASSIFICATION OF CERTAIN PROGRAMS.

It is the sense of Congress that the President should periodically review the level of classification of programs that make use of national security letters (as defined in section 203 of this Act) or the authorities under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) to determine if such programs can be declassified, in whole or in part, without interfering with an ongoing investigation or otherwise threatening national security.

PURPOSE AND SUMMARY

H.R. 3845, the "USA PATRIOT Amendments Act of 2009," introduced by Chairman Conyers, Mr. Nadler, Mr. Scott, Mr. Cohen, Ms. Harman, Ms. Jackson Lee, and Mr. Johnson reauthorizes two expiring provisions of the USA PATRIOT Act of 2001:[1] section 206, regarding roving wiretaps, and section 215, regarding orders for tangible things. This bill gives these provisions a new sunset date of December 31, 2013. It also makes reforms to section 215 authority and to other related surveillance and collection authorities, including national security letters (NSLs), orders for pen register and trap and trace devices for foreign intelligence purposes, and criminal "sneak and peek" search warrants. Moreover, the bill enhances the use of audits and reports dealing with the use and efficacy of these investigative authorities. It does not reauthorize the "Lone Wolf" provision of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA),[2] allowing this provision, which has never been used, to sunset on December 31, 2009. These modifications and reforms seek to ensure that the government can conduct efficient, thorough, and effective national security investigations in a manner that also appropriately protects privacy and civil liberties.

BACKGROUND AND NEED FOR THE LEGISLATION

INTELLIGENCE COLLECTION TOOLS SET TO EXPIRE ON DECEMBER 31, 2009

Section 206—Roving Wiretaps

Section 206 of the USA PATRIOT Act[3] amended the Foreign Intelligence Surveillance Act[4] (FISA) to allow for multipoint or "roving" wiretaps, which permit the government to include multiple surveillance sites associated with a facility authorized in an order of the Foreign Intelligence Surveillance Court (FISC) *if* it can show that the target was taking steps to thwart surveillance. FISA roving authority allows the government to follow a target that switches communication facilities without having to return to court and obtain a new order, thus avoiding the risk of losing valuable foreign intelligence information during the time required to obtain and serve a new court order.

Before the enactment of section 206, the scope of electronic surveillance authorized by a FISC order was limited in two ways. First, the location that was the subject of surveillance had to be identified.[5] Second, only specifically identified third parties could be directed to facilitate electronic surveillance by the government.[6] In cases where the location was unknown, the identity of the person who would need to assist the government could not be specified in the order.[7] Limiting the class of persons who could be directed

---

[1] Pub. L. 107–56.
[2] Pub. L. 108–458.
[3] Pub. L. 107–56, § 206, codified at 50 U.S.C. § 1805(c)(2)(B) (2008).
[4] Pub. L. 95–511.
[5] See 50 U.S.C. § 1805(c)(1)(B) (2001) (requiring FISA warrants to specify the "nature and location of each of the facilities or places at which electronic surveillance will be directed").
[6] See 50 U.S.C. § 1805(c)(2)(B) (2001).
[7] Liu, Amendments to the Foreign Intelligence Surveillance Act Set to Expire in 2009, CRS Report for Congress, March 16, 2009, at 4 (R40138).

to assist the government by a FISC order effectively limited the reach of FISC orders to known and identifiable locations.[8]

Section 206 of the USA PATRIOT Act amended Section 105(c)(2)(B) of FISA to provide that "in circumstances where the Court finds, based on specific facts provided in the application, that the actions of the target of the application may have the effect of thwarting the identification of a specified person," a FISA order may direct "other persons" to assist with the electronic surveillance.[9] In a subsequent technical amendment, the requirement that the order specify the location of the surveillance was also changed, so that it only applied if the facilities or places were known.[10] These modifications had the effect of allowing FISA orders to direct unspecified individuals to assist the government in performing electronic surveillance, thus permitting court orders to authorize surveillance of places or locations that were unknown at the time the order was issued.[11] From a practical standpoint, if the government first establishes that the target of electronic surveillance is a foreign power or agent of a foreign power who is continually switching cell phones in order to thwart surveillance, a roving FISA order allows the government to "follow" and intercept the target on each new cell phone number being used, without having to return to court for a new order directing new individuals to assist the government in performing the surveillance.

The USA PATRIOT Improvement and Reauthorization Act of 2005 further amended section 206 to require that the FISC be notified within 10 days after "surveillance begins to be directed at any new facility or place." [12] Moreover, the FISC must be informed of the nature and location of each new facility or place, the facts and circumstances relied upon to justify the new surveillance, a statement of any proposed minimization procedures that differ from those contained in the original application or order, and the total number of facilities or places subject to surveillance under the authority of the present order.[13]

Notwithstanding the additional roving wiretap notification requirements imposed on the government by the USA PATRIOT Improvement and Reauthorization Act of 2005, various experts have raised concerns that FISA roving authority—specifically in the situation where the government only provides a description (not the actual identity) of a target, and does not identify all of the facilities or places at which electronic surveillance is directed—increases the prospect that the government may intercept communications between individuals who are not FISA targets. In other words, if the government's warrant application need not provide either the actual identity of a target or all of the places and facilities where it will surveil, then the government could end up surveiling multiple unrelated people at multiple places who merely fit the target's description. This potential exists, according to Suzanne Spaulding, former Democratic Staff Director for the U.S. House of Representa-

---

[8] Id.
[9] 50 U.S.C. § 1805(c)(2)(B) (2008).
[10] Pub. L. 107–108, § 314(a)(2)(A).
[11] Liu, Amendments to the Foreign Intelligence Surveillance Act Set to Expire in 2009, CRS Report for Congress, March 16, 2009, at 5 (R40138).
[12] 50 U.S.C. § 1805(c)(3) (2008). This deadline for notification can be extended to up to 60 days by the FISC upon a showing of good cause.
[13] Id.

tives Permanent Select Committee on Intelligence and an Assistant General Counsel at the CIA, because of what she describes generally as "less rigorous" statutory standards for FISA roving warrants than those governing issuance of roving wiretap warrants in criminal investigations under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986.[14]

For example, FISA permits the government to provide "a description of the target" if the identity is not known, where Title III roving applications must definitively identify the target of surveillance.[15] Moreover, Title III explicitly limits an order authorizing or approving "roving" interceptions to "such time as it is reasonable to presume" that the person identified in the application is "reasonably proximate" to the communication instrument. Title III also differs from FISA roving authority by requiring that the target be notified of surveillance, generally 90 days after the surveillance ends.[16] While such notification is understandably absent in the FISA context, this requirement and other explicit Title III roving elements not present in FISA roving authority reduce the likelihood that communications between unrelated persons would be intercepted.[17] Ms. Spaulding, former representative Tom Evans (R-DE), and Mike German, Policy Counsel for the American Civil Liberties Union and former FBI Agent, all witnesses at the September 22, 2009, Subcommittee hearing on the USA PATRIOT Act, urged this Committee to consider "tightening" statutory language, so as to require a FISA judge to determine that the target has been described with sufficient particularity to distinguish the target from other potential users of the instrument or facility being surveilled.[18]

The Committee added language to section 105(c)(2)(B), the FISA roving wiretap provision (50 U.S.C. § 1805(c)(2)(B)), to clarify Congressional intent that the government must describe its roving target with a sufficient degree of particularity to allow a judge to be able to distinguish the target from other potential users of places or facilities to be surveilled. This language is not intended to change current practice. With these modifications, section 206 is reauthorized until December 31, 2013.

Section 6001(a) of IRTPA—Lone Wolf

Commonly referred to as the "Lone Wolf" provision, § 6001(a) of the Intelligence Reform and Terrorism Protection Act (IRTPA), broadened the definition of individuals who could be FISA targets. It permitted surveillance of non-U.S. persons preparing to engage in or engaging in international terrorism, without requiring evidence linking those persons to an identifiable foreign power or terrorist organization.[19] This provision was created in response to the

[14] Pub. L. 99–508 § 106(d)(3), codified at 18 U.S.C. 2518(11) (2008).
[15] Hearing on the USA PATRIOT Act before the House Judiciary Subcomm. on the Constitution, Civil Rights, and Civil Liberties, 111th Cong. (2009) (written statement of Suzanne Spaulding).
[16] Id.
[17] Id.
[18] Hearing on the USA PATRIOT Act before the House Judiciary Subcomm. on the Constitution, Civil Rights, and Civil Liberties, 111th Cong. (2009) (written statements of Suzanne Spaulding, former Rep. Tom Evans, and Mike German).
[19] Pub. L. 108–458 § 6001(a).

FBI's attempt to obtain a FISA order to search the laptop of Zacarias Moussaoui in October, 2001. The FBI believed it had insufficient information to demonstrate that Moussaoui was an agent of a foreign power, as required by FISA at the time, although the term "foreign power" included international terrorist groups.[20] The FISA Amendments Act of 2008 further expanded the definition of "Lone Wolf" to include any non-United States person who engages in or prepares to engage in the international proliferation of weapons of mass destruction, without requiring evidence linking those persons to an identifiable foreign power or terrorist organization.[21]

Critics of the Lone Wolf provision argue that it undermines the constitutional justification for the entire FISA statute: that the extraordinary FISA powers used by our government are constitutional only because they are used against our most serious adversaries, foreign governments and organized foreign powers. Accordingly, these critics assert that expanding the reach of the statute to individuals acting alone puts the whole FISA statute at risk.[22] Moreover, critics argue Lone Wolf can safely be allowed to expire, because a traditional Title III warrant can be obtained against any individual who fits the definition of Lone Wolf.[23] Indeed, Title III warrants must be used to investigate equally dangerous domestic terrorists, as Lone Wolf does not apply to United States persons.

Todd Hinnen, Deputy Assistant Attorney General for the Justice Department's National Security Division, testified in a hearing before the Subcommittee on the Constitution, Civil Rights, and Civil Liberties that the Lone Wolf provision has never been used.[24] This admission further demonstrates that Lone Wolf is not so essential that the inherent compromise of civil liberties it represents should be allowed to persist in American law. The bill, therefore, does not reauthorize Lone Wolf.

Section 215 Orders—Tangible Evidence Procurement

Section 215 of the USA PATRIOT Act allows the government to obtain a FISA order requiring private parties to produce "tangible things" such as business records that are relevant to foreign intelligence, counterterrorism, or counterintelligence investigations.[25] To issue such an order, the FISA judge or appropriately designated magistrate judge[26] need only find that the FBI has made "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such

---

[20] Liu, "Amendments to the Foreign Intelligence Surveillance Act Set to Expire in 2009," CRS Report for Congress, March 16, 2009 at 3 (R40138).

[21] Pub. L. 110–261 § 110.

[22] Hearing on the USA PATRIOT Act before the House Judiciary Subcomm. on the Constitution, Civil Rights, and Civil Liberties, 111th Cong. (2009) (written statement of Suzanne Spaulding).

[23] Id.

[24] Id. (testimony of Todd Hinnen).

[25] 50 U.S.C. § 1861(a)(1). Section 1861 is titled, "Access to certain business records for foreign intelligence and international terrorism investigations," suggesting that the "tangible things" it describes may only be of the business sort. However, titles of statutes (or their subsections) are traditionally of weak interpretive value to courts.

[26] United States Magistrate Judges (under chapter 43 of title 28) can be publicly designated by the Chief Justice of the United States to have the power hear applications and grant orders for the production of tangible things. See 50 U.S.C. § 1861(b)(1)(B).

investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment."[27] Upon such finding, the order must issue.[28] Such orders may not disclose their purpose,[29] however, and those receiving them may not disclose their existence.[30] This last provision is often referred to as a "gag rule."

In support of reauthorization of section 215, the Department of Justice has represented that, based on its operational experience, there will continue to be instances in which FBI investigators need to obtain transactional information that does not fall within the scope of authorities relating to NSLs, and where they must operate in an environment that precludes the use of less secure criminal authorities.[31] DOJ further indicates that for the period 2004–2007, the FISC issued about 220 orders to produce business records.[32] Of these, 173 orders were issued in 2004–2006 in combination with FISA pen register orders to address an anomaly in the statutory language that prevented the acquisition of subscriber information ordinarily associated with pen register information.[33] Congress corrected this deficiency in the pen register provision in 2006 in the USA PATRIOT Improvement and Reauthorization Act, making this use of business records authority unnecessary.[34] The remaining business records orders issued between 2004 and 2007 were used to obtain transactional information that did not fall within the scope of any other national security investigative authority (such as an NSL).[35] Some of these orders were used to support sensitive intelligence collections.[36]

In 1998, Congress first amended FISA to provide access to certain records that were not available through NSLs. Specifically, new section 501 created a mechanism for Federal investigators to compel the production of records from common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities.[37] The FISC would issue an order if, among other things, the application contained "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[38]

In 2001, section 215 of the USA PATRIOT Act made several changes to the procedures under section 501 of FISA for obtaining business records.[39] Prior to enactment of the USA PATRIOT Act, only records from four specific categories of businesses could be obtained. Section 215 expanded the scope to "any tangible things."[40]

The expanded scope produced strong opposition from the library community, to the degree that section 215 came to be known by some as the "library provision." The opposition stemmed mainly

---

[27] 50 U.S.C. § 1861(b)(2)(A).
[28] 50 U.S.C. § 1861(c)(1) ("[I]f the judge finds that the application meets the requirements of subsections (a) and (b) of this section, the judge *shall* enter an ex parte order as requested, or as modified, approving the release of tangible things." (emphasis added)).
[29] 50 U.S.C. § 1861(c)(2)(E).
[30] 50 U.S.C. § 1861(d).
[31] Department of Justice letter to the Honorable Patrick J. Leahy (September 14, 2009).
[32] Id.
[33] Id.
[34] Id.
[35] Id.
[36] Id.
[37] 50 U.S.C. § 1861(a) (2001).
[38] 50 U.S.C. § 1861(b)(2)(B) (2001).
[39] Pub. L. 107–56, codified at 50 U.S.C. § 1862(a)–(b) (2008).
[40] 50 U.S.C. § 1861(a)(1) (2008).

from the chilling effect such access could have on the exercise of First Amendment rights and purported intrusions into areas protected by the Fourth Amendment.[41] In response to these concerns, the USA PATRIOT Improvement and Reauthorization Act of 2005 added a requirement that the application for a section 215 order has to be approved by the FBI Director, Deputy Director, or Executive Assistant Director for National Security, if the application seeks "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."[42]

Section 215 of the USA PATRIOT Act also modified the standard for issuance of a "tangible things" order. Prior to the enactment of section 215, the government had to make a showing of "specific and articulable facts giving reasons to believe that the person to whom the records pertain[ed] is a foreign power or an agent of a foreign power."[43] Under section 215 as originally enacted in the USA PATRIOT Act, by contrast, the applicant only needed to "specify that the records concerned [were] sought for an authorized [foreign intelligence, counterterrorism, or counterintelligence] investigation."[44] In 2005, Congress further amended section 215 to require "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized [foreign intelligence, counterterrorism, or counterintelligence] investigation."[45] Records are presumptively relevant if they pertain to (1) a foreign power or agent of a foreign power; (2) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (3) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation.[46]

Orders issued under section 215 are accompanied by automatic nondisclosure orders, or gag orders, prohibiting the recipients from disclosing that the FBI has sought or obtained tangible things pursuant to a FISA order. The recipient may only discuss the order with other persons as necessary to comply with the order, with an attorney to obtain legal advice or assistance, or with other persons the FBI permits.[47]

In addition to modifying the standard for issuance, The USA PATRIOT Improvement and Reauthorization Act of 2005 provided procedures for recipients of section 215 orders to obtain judicial review of orders compelling the production of business records.[48] Once a petition for review is submitted by a recipient, a FISA judge must determine within 72 hours whether the petition is frivolous.[49] If the petition is frivolous, it must be denied and the order affirmed.[50] The order may be modified or set aside if it does not meet the requirements of FISA or is otherwise unlawful.[51] Appeals by ei-

---

[41] Liu, "Amendments to the Foreign Intelligence Surveillance Act Set to Expire in 2009," CRS Report for Congress, March 16, 2009, at 8 (R40138).
[42] 50 U.S.C. § 1861(a)(3) (2008).
[43] 50 U.S.C. § 1861(b)(2)(B) (2001).
[44] Pub. L. 107–56 § 215.
[45] Pub. L. 109–177 § 106(b).
[46] Id.
[47] 50 U.S.C. § 1861(d)(1) (2008).
[48] 50 U.S.C. § 1861(f)(2)(A)(i) (2008).
[49] 50 U.S.C. § 1861(f)(2)(A)(ii) (2008).
[50] Id.
[51] 50 U.S.C. § 1861(f)(2)(B) (2008).

ther party may be heard by the Foreign Intelligence Court of Review and the Supreme Court.[52]

A recipient must wait 1 year from the date of the section 215 production order to appeal an associated nondisclosure or "gag" order.[53] However, if a high level government official (to include the Attorney General, the Deputy Attorney General, an Assistant Attorney General or the Director of the FBI) certifies that disclosure may endanger the national security of the United States, such certification is treated as conclusive, thus automatically defeating the recipient's challenge, unless a judge finds that the certification was made in bad faith.[54]

As the law has evolved from the requirement that the government demonstrate "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power" to the more permissive standard requiring only "relevance to an authorized investigation," and as section 215 has broadened the scope of section 501 of FISA from records of four specific types of businesses to an ability to acquire "any tangible thing," this Committee has reconsidered the appropriateness of such an expansive collection tool. This collection authority, for example, currently allows the government to acquire lists of what library patrons are reading merely by showing relevance to an authorized investigation. We have heard from experts who caution that while such broad language may sometimes be appropriate for the wide-ranging nature of intelligence collection, it provides greater opportunity for abuses and mistakes.[55] Moreover, because section 215 orders come with compulsory nondisclosure or "gag orders," such abuses are not easily discovered.

These concerns must be evaluated, however, with the understanding that, unlike the government's use of NSLs, which requires no court order, the government obtains a section 215 order from a court. Recognizing the inherent protections provided by court review, the Committee amends the law to require the government to provide a statement of facts and circumstances relied upon by the applicant to justify the applicant's belief that the tangible things sought are relevant to the authorized investigation. This modification will strengthen judicial oversight by ensuring that the government is presenting a thorough statement of facts for review. The bill further strengthens judicial oversight by eliminating the "conclusive certification" by a high-level government official that automatically defeats a challenge to a section 215 gag order. The bill also permits these gag orders to be challenged immediately, removing the 1-year delay under current law. Additional oversight of section 215 is facilitated though DOJ Inspector General reports mandated by the bill, and a new sunset date of December 31, 2013.

The Committee has particular civil liberties concerns with a such a broad collection standard as it applies to personally identifiable information concerning the use of libraries and purchases from booksellers. Indeed, core First Amendment activities such as reading require careful protection from government intrusion. The Com-

[52] 50 U.S.C. § 1861(f)(3) (2008).
[53] 50 U.S.C. § 1861(f)(2)(A)(i) (2008).
[54] 50 U.S.C. § 1861(f)(2)(C)(ii) (2008).
[55] Hearing on the USA PATRIOT Act before the House Judiciary Subcomm. on the Constitution, Civil Rights, and Civil Liberties, 111th Cong. (2009) (written statement of Suzanne Spaulding).

mittee has seen no evidence that such a broad standard to permit general collection of information about whatever people are reading is warranted.

At the same time, the Committee recognizes that there may be specific factual circumstances in a particular investigation where it could be necessary for the government to obtain access to such records. To avoid prohibiting access where justified by a specific, particularized need, the bill amends the law to allow access if the government can meet a heightened standard of "specific and articulable facts" showing that there are reasonable grounds to believe that the records sought are "relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities" *and* "(I) pertain to a foreign power or 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 who is the subject of such authorized investigation."

The Committee also recognizes that some "mixed purchase" records may contain information that falls both inside and outside of the heightened standard pertaining to libraries or bookseller information. For example, a single purchase at a modern superstore may include books and journals, as well as bomb-making materials. The Committee does not intend for the heightened library/bookseller information standard to apply to information that would otherwise be governed by the general section 215 "tangible things" standard merely because such information happens to be co-mingled with library/bookseller information in the same records.

As previously indicated, section 215 orders are used to support sensitive collections. In an effort to ensure that appropriate consideration is given to civil liberties protections with respect to these intelligence collections, the bill calls for the President to report to Congress on whether the procedures for these collections could be further modified so as to enhance civil liberties protections without undermining national security objectives.

With these modifications, the bill reauthorizes section 215 with a new sunset date of December 31, 2013.

NATIONAL SECURITY LETTER REFORM

National security letters (NSLs) are written directives for information issued by the FBI in national security investigations to third-party companies such as telephone companies, financial institutions, Internet service providers, and consumer credit agencies, without judicial review. Unlike section 215 "tangible things" orders, the FBI issues NSLs without any judicial authorization or review. Over the last 20 years, Congress has enacted a series of laws authorizing the FBI to use NSLs to obtain information in terrorism, espionage, and classified information leak investigations without obtaining warrants from the Foreign Intelligence Surveillance Court or approval from another court.

There are five provisions of law that authorize the FBI to issue five types of NSLs: (1) the Right to Financial Privacy Act (RFPA)

(to obtain financial institution customer records);[56] (2) the Electronic Communications Privacy Act (ECPA) (to obtain certain communication service provider records);[57] (3) the Fair Credit Reporting Act (FCRA) (to obtain certain financial information records);[58] (4) FCRA (to obtain credit agency consumer records for counterterrorism investigations);[59] and (5) the National Security Act (NSA) (to obtain financial information, records, and consumer reports).[60] Companies receiving NSLs are usually prohibited, based on "gag" orders that accompany such NSLs, from disclosing publically the fact or nature of a request.

Prior to the enactment of the USA PATRIOT Act, the standard for issuing an NSL required that the information sought was relevant to an authorized counterterrorism or counterintelligence investigation *and* that there were specific and articulable facts giving reason to believe that the information sought pertained to a foreign power or agent of a foreign power. The USA PATRIOT Act modified that standard to require only that the records be relevant to an authorized counterterrorism or counterintelligence investigation—provided that such investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution.

With the relaxing of the NSL standard to simple "relevance" to an authorized investigation, civil liberties and privacy experts maintain that NSLs allow the government to access, far too readily, personal information about people who are not known or even suspected to have done anything wrong.[61] Moreover, while the USA PATRIOT Improvement and Reauthorization Act of 2005 allowed NSL recipients to consult a lawyer, NSLs and related gag orders remain free from any meaningful judicial review.[62] Indeed, the Second Circuit, in *Doe v. Mukasey,* 549 F.3d 861 (2008), found various constitutional defects in nondisclosure orders pertaining to NSLs.

Critics of NSLs also argue that the broad USA PATRIOT Act standard for issuance invites potential abuse, an argument bolstered by reports from DOJ's Office of the Inspector General (OIG). The 2007 and 2008 OIG Reports regarding the FBI's use of NSLs revealed abuses including: (1) gathering irrelevant private information about individuals and uploading and indefinitely retaining it in FBI databases; (2) inaccurate reporting to Congress regarding the number and use of NSLs; (3) issuing NSLs without proper authorization and outside statutory and regulatory requirements; and (4) widespread abuse in the use of so-called "exigent letters"—"emergency" requests for telephone and other data—in non-emergencies, without even a pending investigation, as a means to bypass normal NSL procedures.[63]

OIG also found one instance in which the FBI had issued NSLs for information after the FISC had refused to issue section 215 or-

---

[56] Section 1114(a)(5)(A),12 U.S.C. 3414(a)(5)(A).
[57] 18 U.S.C. § 2709(a).
[58] Section 626, 15 U.S.C. 1681u.
[59] Section 627, 15 U.S.C. 1681v.
[60] Section 802, 50 U.S.C. 436.
[61] Hearing on the USA PATRIOT Act before the House Judiciary S. Comm. on the Constitution, Civil Rights, and Civil Liberties, 111th Cong. (2009) (written statement of Mike German on behalf of the American Civil Liberties Union).
[62] Id.
[63] See generally Dep't of Justice, Ofc. of Inspector General, A Review of the Federal Bureau of Investigation's Use of National Security Letters, available at http://www.npr.org/documents/2007/mar/doj/doj__oig__nsl.pdf (March 2007).

ders for the same information, citing First Amendment concerns.[64] OIG "questioned the appropriateness" of the FBI's issuing these NSLs after the court's decision, because NSLs have the same First Amendment caveat as Section 215 requests and the FBI issued the NSLs based on the same factual predicate.[65] The FBI issued the NSLs without further review of the underlying investigation to ensure that it was not premised solely on protected First Amendment conduct.[66]

In testimony before the Constitution Subcommittee hearing on the USA PATRIOT Act this September, ACLU Policy Counsel Mike German and former Representative Tom Evans urged the Committee to: (1) change the issuance standard for NSLs to ensure that the government is seeking information on the appropriate individuals; and (2) address concerns regarding NSL gag orders, and provide meaningful judicial review of both NSLs and associated gag orders.[67]

The Committee has examined these concerns and balanced them against the government's need to acquire basic "building block" information in national security investigations in an efficient manner. Because the government can issue NSLs without obtaining court authorization, it is appropriate to tie the NSL issuance standard more closely to information pertaining to a foreign power or agent of a foreign power—terms that are well-defined in the law. The bill therefore requires the government to produce and retain, prior to the issuance of an NSL, a statement of "specific and articulable" facts documenting how the information sought is relevant to an authorized counterterrorism or counterintelligence investigation and: (1) pertains to a foreign power or agent of a foreign power; (2) is relevant to the activities of a suspected agent of a foreign power or agent of a foreign power that is the subject of such authorized investigation; or (3) pertains to an individual in contact with, or personally known to, a suspected agent of a foreign power that is the subject of such authorized investigation.

The bill also corrects constitutional defects in the issuance of NSL nondisclosure orders identified by the Second Circuit in *Doe v. Mukasey,* and adopts procedures suggested by the court for a constitutionally sound process. These procedures include: (1) requiring the government to notify the recipient of a right to judicial review of a nondisclosure order at the time the government serves the NSL on the recipient; (2) requiring the government to seek a court order prohibiting disclosure within thirty (30) days of being notified by the recipient that the recipient wants a court to review the nondisclosure requirement associated with the NSL; and (3) requiring the government to seek court renewals of nondisclosure orders every 180 days (or less where justified by the timeframe established by the court's order). Moreover, the bill eliminates the "conclusive certifications" that previously allowed certain high-level government officials to make national security-related certifications

---

[64] Written Statement of Glenn Fine, Inspector General, Dep't of Justice, Hearing on "The FBI's Use of National Security Letters and Section 215 Orders for Business Records," before the Subcommittee on Constitution, Civil Rights, and Civil Liberties, April 15, 2008.

[65] Id.

[66] Id.

[67] Hearing on the USA PATRIOT Act before the House Judiciary Subcomm. on the Constitution, Civil Rights, and Civil Liberties, 111th Cong. (2009) (written statements of Mike German and former Rep. Tom Evans).

that, unless made in bad faith, would automatically defeat a challenge to a nondisclosure order.

OVERSIGHT, CIVIL LIBERTIES AND PRIVACY PROTECTIONS

In an effort to enhance civil liberties and privacy protections, this Committee examined ways to increase Judicial, Legislative, and Executive Branch oversight in relation to collection and surveillance authorities, and to require increased public reporting of the use of these authorities in a manner that will not otherwise threaten national security. Section 301 of the bill expresses a sense of Congress that the President should periodically review the level of classification of programs that make use of NSLs or FISA authorities, to determine if such programs can be declassified, in whole or in part, without interfering with ongoing investigations or otherwise threatening national security. Sections 108 and 209 of the bill require public reporting pertaining to FISA and NSLs.

Substantively, for the first time in statute, the bill addresses the need, in appropriate circumstances, for minimization procedures pertaining to information acquired from NSLs and FISA pen register and trap-and-trace devices. The bill also strengthens judicial oversight of FISA pen/trap and section 215 "tangible things" orders, by underscoring a FISA judge's authority to review compliance with minimization procedures. Moreover, under section 107 of the bill, in order to obtain an order authorizing the use of a FISA pen/trap, the government would now provide a statement of facts justifying the applicant's belief that the information likely to be obtained is relevant, rather than merely certifying such relevance. The bill also strengthens judicial oversight of criminal "sneak and peek" warrants by shortening the periods of time for which the government can delay notice of a search before having to go back to the court for continued authorization of the delay of notice.

HEARINGS

The Committee's Subcommittee on Constitution, Civil Rights, and Civil Liberties held a hearing on the USA PATRIOT Act on September 22, 2009. Witnesses at the hearing included Todd Hinnen, Deputy Assistant Attorney General, National Security Division; Suzanne Spalding, Principal, Bingham Consulting Group, and former Democratic Staff Director, U.S. House Permanent Select Committee on Intelligence; Mike German, Policy Counsel, ACLU and former FBI Agent; Thomas B. Evans, Jr., Chairman, The Evans Group, Ltd. and former Member of Congress (R-DE); and Kenneth Wainstein, Partner, O'Melveny & Myers, LLP and former Assistant Attorney General, National Security Division.

On October 29, 2009, the Committee held a classified hearing on the USA PATRIOT Act and related matters. Witnesses at that hearing included David S. Kris, Assistant Attorney General for National Security, Department of Justice and Michael E. Leiter, Director, National Counterterrorism Center.

The were also two hearings held in the 110th Congress. On April 15, 2008, the Subcommittee on the Constitution, Civil Rights, and Civil Liberties held a hearing on H.R. 3189 (110th), the "National Security Letters Reform Act of 2007." Witnesses included Glenn A. Fine, Inspector General, U.S. Department of Justice; Valerie

Caproni, General Counsel, Federal Bureau of Investigation; Jameel Jaffer, Director, National Security Project, American Civil Liberties Union; Bruce Fein, Lichfield Group, Inc.; Michael J. Woods, Former Chief, FBI National Security Law Unit; and David Kris, Former Associate Deputy Attorney General, U.S. Department of Justice.

On March 20, 2007, the Committee held a hearing on The Inspector General's Independent Report on the FBI's Use of National Security Letters. Witnesses included Valerie Caproni, General Counsel, Office of General Counsel, Federal Bureau of Investigation, and Glenn A. Fine, Inspector General, U.S. Department of Justice.

COMMITTEE CONSIDERATION

On November 4 and 5, 2009, the Committee met in open session for consideration of H.R. 3485. On November 5, 2009, the Committee ordered the bill H.R. 3845 favorably reported with amendment, by voice vote, a quorum being present.

COMMITTEE VOTES

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the Committee advises that the following rollcall votes occurred during the Committee's consideration of H.R. 3845:

1. An amendment by Mr. Gallegly (to the manager's amendment and the bill) to strike additional section 215 business records protections for libraries and bookseller information. Defeated 21 to 13.

ROLLCALL NO. 1

	Ayes	Nays	Present
Mr. Conyers, Jr., Chairman		X	
Mr. Berman			
Mr. Boucher		X	
Mr. Nadler		X	
Mr. Scott		X	
Mr. Watt		X	
Ms. Lofgren		X	
Ms. Jackson Lee		X	
Ms. Waters		X	
Mr. Delahunt			
Mr. Wexler		X	
Mr. Cohen		X	
Mr. Johnson		X	
Mr. Pierluisi		X	
Mr. Quigley		X	
Ms. Chu		X	
Mr. Gutierrez		X	
Ms. Baldwin		X	
Mr. Gonzalez		X	
Mr. Weiner		X	
Mr. Schiff		X	
Ms. Sánchez			
Ms. Wasserman Schultz		X	
Mr. Maffei		X	
Mr. Smith, Ranking Member	X		
Mr. Sensenbrenner, Jr.			
Mr. Coble	X		
Mr. Gallegly	X		
Mr. Goodlatte	X		
Mr. Lungren	X		

ROLLCALL NO. 1—Continued

	Ayes	Nays	Present
Mr. Issa	X		
Mr. Forbes	X		
Mr. King			
Mr. Franks	X		
Mr. Gohmert	X		
Mr. Jordan	X		
Mr. Poe	X		
Mr. Chaffetz	X		
Mr. Rooney			
Mr. Harper	X		
Total	13	21	

2. An amendment by Mr. Lungren (to the manager's amendment and the bill) to strike minimization procedures for NSLs. Defeated 18 to 8.

ROLLCALL NO. 2

	Ayes	Nays	Present
Mr. Conyers, Jr., Chairman		X	
Mr. Berman		X	
Mr. Boucher		X	
Mr. Nadler		X	
Mr. Scott		X	
Mr. Watt		X	
Ms. Lofgren		X	
Ms. Jackson Lee			
Ms. Waters			
Mr. Delahunt			
Mr. Wexler		X	
Mr. Cohen		X	
Mr. Johnson		X	
Mr. Pierluisi			
Mr. Quigley		X	
Ms. Chu		X	
Mr. Gutierrez		X	
Ms. Baldwin		X	
Mr. Gonzalez		X	
Mr. Weiner		X	
Mr. Schiff		X	
Ms. Sánchez			
Ms. Wasserman Schultz		X	
Mr. Maffei			
Mr. Smith, Ranking Member	X		
Mr. Sensenbrenner, Jr.			
Mr. Coble			
Mr. Gallegly			
Mr. Goodlatte			
Mr. Lungren	X		
Mr. Issa	X		
Mr. Forbes	X		
Mr. King			
Mr. Franks	X		
Mr. Gohmert			
Mr. Jordan			
Mr. Poe			
Mr. Chaffetz	X		
Mr. Rooney	X		
Mr. Harper	X		
Total	8	18	

3. An amendment by Mr. Chaffetz (to the manager's amendment and the bill) to strike the "specific and articulable" facts requirement for NSLs and replace it with a requirement for facts showing relevance to an authorized investigation to protect against international terrorism or clandestine intelligence activities. Defeated 18 to 11.

ROLLCALL NO. 3

	Ayes	Nays	Present
Mr. Conyers, Jr., Chairman		X	
Mr. Berman		X	
Mr. Boucher			
Mr. Nadler		X	
Mr. Scott		X	
Mr. Watt		X	
Ms. Lofgren		X	
Ms. Jackson Lee			
Ms. Waters		X	
Mr. Delahunt			
Mr. Wexler			
Mr. Cohen		X	
Mr. Johnson		X	
Mr. Pierluisi		X	
Mr. Quigley		X	
Ms. Chu		X	
Mr. Gutierrez			
Ms. Baldwin		X	
Mr. Gonzalez		X	
Mr. Weiner		X	
Mr. Schiff		X	
Ms. Sánchez			
Ms. Wasserman Schultz		X	
Mr. Maffei		X	
Mr. Smith, Ranking Member	X		
Mr. Sensenbrenner, Jr.	X		
Mr. Coble	X		
Mr. Gallegly			
Mr. Goodlatte			
Mr. Lungren	X		
Mr. Issa	X		
Mr. Forbes	X		
Mr. King	X		
Mr. Franks	X		
Mr. Gohmert			
Mr. Jordan			
Mr. Poe			
Mr. Chaffetz	X		
Mr. Rooney	X		
Mr. Harper	X		
Total	11	18	

4. A manager's amendment by Mr. Conyers to make a number of clarifying refinements. Agreed to 19 to 11.

ROLLCALL NO. 4

	Ayes	Nays	Present
Mr. Conyers, Jr., Chairman	X		
Mr. Berman	X		
Mr. Boucher	X		
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		

ROLLCALL NO. 4—Continued

	Ayes	Nays	Present
Ms. Lofgren	X		
Ms. Jackson Lee			
Ms. Waters	X		
Mr. Delahunt			
Mr. Wexler	X		
Mr. Cohen	X		
Mr. Johnson	X		
Mr. Pierluisi	X		
Mr. Quigley	X		
Ms. Chu	X		
Mr. Gutierrez			
Ms. Baldwin	X		
Mr. Gonzalez			
Mr. Weiner	X		
Mr. Schiff	X		
Ms. Sánchez			
Ms. Wasserman Schultz	X		
Mr. Maffei	X		
Mr. Smith, Ranking Member		X	
Mr. Sensenbrenner, Jr.		X	
Mr. Coble		X	
Mr. Gallegly			
Mr. Goodlatte			
Mr. Lungren		X	
Mr. Issa		X	
Mr. Forbes		X	
Mr. King		X	
Mr. Franks		X	
Mr. Gohmert			
Mr. Jordan			
Mr. Poe			
Mr. Chaffetz		X	
Mr. Rooney		X	
Mr. Harper		X	
Total	19	11	

5. An amendment by Mr. Schiff to (1) replace the "specific and articulable" facts requirement for a section 215 order with "statement of facts," (2) strike the presumptive relevance for documents that pertain to a foreign power or agent, the activities of a suspected agent of a foreign power, who is the subject of the authorized investigation, or an individual in contact with, or known to, the suspected agent, and (3) require the President to report to Congress regarding whether certain operations authorized by Section 215 could be appropriately modified so as to enhance civil liberties protections. Agreed to 19 to 12.

ROLLCALL NO. 5

	Ayes	Nays	Present
Mr. Conyers, Jr., Chairman	X		
Mr. Berman	X		
Mr. Boucher	X		
Mr. Nadler	X		
Mr. Scott	X		
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee			
Ms. Waters	X		
Mr. Delahunt			

ROLLCALL NO. 5—Continued

	Ayes	Nays	Present
Mr. Wexler	X		
Mr. Cohen	X		
Mr. Johnson	X		
Mr. Pierluisi	X		
Mr. Quigley	X		
Ms. Chu	X		
Mr. Gutierrez			
Ms. Baldwin	X		
Mr. Gonzalez			
Mr. Weiner	X		
Mr. Schiff	X		
Ms. Sánchez			
Ms. Wasserman Schultz	X		
Mr. Maffei	X		
Mr. Smith, Ranking Member		X	
Mr. Sensenbrenner, Jr.			
Mr. Coble		X	
Mr. Gallegly			
Mr. Goodlatte		X	
Mr. Lungren		X	
Mr. Issa		X	
Mr. Forbes		X	
Mr. King		X	
Mr. Franks		X	
Mr. Gohmert			
Mr. Jordan			
Mr. Poe		X	
Mr. Chaffetz		X	
Mr. Rooney		X	
Mr. Harper		X	
Total	19	12	

6. An amendment by Mr. Lungren (to the amendment by Mr. Schiff) restoring the "presumptive relevance" standard for certain documents sought under section 215. Defeated 19 to 13.

ROLLCALL NO. 6

	Ayes	Nays	Present
Mr. Conyers, Jr., Chairman		X	
Mr. Berman		X	
Mr. Boucher		X	
Mr. Nadler		X	
Mr. Scott		X	
Mr. Watt		X	
Ms. Lofgren		X	
Ms. Jackson Lee			
Ms. Waters		X	
Mr. Delahunt			
Mr. Wexler		X	
Mr. Cohen		X	
Mr. Johnson		X	
Mr. Pierluisi		X	
Mr. Quigley		X	
Ms. Chu		X	
Mr. Gutierrez			
Ms. Baldwin		X	
Mr. Gonzalez			
Mr. Weiner		X	
Mr. Schiff		X	
Ms. Sánchez			
Ms. Wasserman Schultz		X	

ROLLCALL NO. 6—Continued

	Ayes	Nays	Present
Mr. Maffei		X	
Mr. Smith, Ranking Member	X		
Mr. Sensenbrenner, Jr.	X		
Mr. Coble	X		
Mr. Gallegly			
Mr. Goodlatte	X		
Mr. Lungren	X		
Mr. Issa	X		
Mr. Forbes	X		
Mr. King	X		
Mr. Franks	X		
Mr. Gohmert			
Mr. Jordan			
Mr. Poe	X		
Mr. Chaffetz	X		
Mr. Rooney	X		
Mr. Harper	X		
Total	13	19	

7. An amendment by Mr. Smith to reauthorize "Lone Wolf" until December 31, 2013. Defeated 15 to 15.

ROLLCALL NO. 7

	Ayes	Nays	Present
Mr. Conyers, Jr., Chairman		X	
Mr. Berman		X	
Mr. Boucher			
Mr. Nadler		X	
Mr. Scott		X	
Mr. Watt		X	
Ms. Lofgren		X	
Ms. Jackson Lee			
Ms. Waters		X	
Mr. Delahunt			
Mr. Wexler		X	
Mr. Cohen			
Mr. Johnson			
Mr. Pierluisi		X	
Mr. Quigley	X		
Ms. Chu		X	
Mr. Gutierrez			
Ms. Baldwin		X	
Mr. Gonzalez		X	
Mr. Weiner		X	
Mr. Schiff	X		
Ms. Sánchez			
Ms. Wasserman Schultz		X	
Mr. Maffei		X	
Mr. Smith, Ranking Member	X		
Mr. Sensenbrenner, Jr.	X		
Mr. Coble	X		
Mr. Gallegly	X		
Mr. Goodlatte	X		
Mr. Lungren			
Mr. Issa	X		
Mr. Forbes	X		
Mr. King			
Mr. Franks	X		
Mr. Gohmert			
Mr. Jordan	X		
Mr. Poe	X		

ROLLCALL NO. 7—Continued

	Ayes	Nays	Present
Mr. Chaffetz	X		
Mr. Rooney	X		
Mr. Harper	X		
Total	15	15	

8. An amendment by Mr. Rooney to strike changes to the standard for issuance of a criminal pen register and trap-and-trace device. Defeated 12 to 10.

ROLLCALL NO. 8

	Ayes	Nays	Present
Mr. Conyers, Jr., Chairman			
Mr. Berman		X	
Mr. Boucher			
Mr. Nadler			
Mr. Scott		X	
Mr. Watt		X	
Ms. Lofgren			
Ms. Jackson Lee		X	
Ms. Waters		X	
Mr. Delahunt			
Mr. Wexler			
Mr. Cohen		X	
Mr. Johnson	X		
Mr. Pierluisi	X		
Mr. Quigley	X		
Ms. Chu		X	
Mr. Gutierrez		X	
Ms. Baldwin		X	
Mr. Gonzalez			
Mr. Weiner		X	
Mr. Schiff	X		
Ms. Sánchez			
Ms. Wasserman Schultz		X	
Mr. Maffei		X	
Mr. Smith, Ranking Member	X		
Mr. Sensenbrenner, Jr.			
Mr. Coble	X		
Mr. Gallegly			
Mr. Goodlatte			
Mr. Lungren	X		
Mr. Issa	X		
Mr. Forbes	X		
Mr. King			
Mr. Franks			
Mr. Gohmert			
Mr. Jordan			
Mr. Poe			
Mr. Chaffetz			
Mr. Rooney	X		
Mr. Harper			
Total	10	12	

9. An amendment by Mr. Lungren to require a court, when reviewing a section 215 nondisclosure order, to give "substantial weight" to a certification by a high-level government official that disclosure may endanger the national security of the United States or interfere with diplomatic relations. Defeated 11 to 8.

ROLLCALL NO. 9

	Ayes	Nays	Present
Mr. Conyers, Jr., Chairman			
Mr. Berman			
Mr. Boucher			
Mr. Nadler			
Mr. Scott		X	
Mr. Watt		X	
Ms. Lofgren		X	
Ms. Jackson Lee		X	
Ms. Waters			
Mr. Delahunt			
Mr. Wexler			
Mr. Cohen		X	
Mr. Johnson		X	
Mr. Pierluisi	X		
Mr. Quigley	X		
Ms. Chu		X	
Mr. Gutierrez			
Ms. Baldwin		X	
Mr. Gonzalez			
Mr. Weiner		X	
Mr. Schiff	X		
Ms. Sánchez			
Ms. Wasserman Schultz		X	
Mr. Maffei		X	
Mr. Smith, Ranking Member	X		
Mr. Sensenbrenner, Jr.			
Mr. Coble			
Mr. Gallegly			
Mr. Goodlatte			
Mr. Lungren	X		
Mr. Issa	X		
Mr. Forbes			
Mr. King			
Mr. Franks	X		
Mr. Gohmert			
Mr. Jordan			
Mr. Poe			
Mr. Chaffetz			
Mr. Rooney	X		
Mr. Harper			
Total	8	11	

10. An amendment by Mr. Issa to modify the standards for "sneak and peek" authority. Agreed to 16 to 10.

ROLLCALL NO. 10

	Ayes	Nays	Present
Mr. Conyers, Jr., Chairman	X		
Mr. Berman			
Mr. Boucher			
Mr. Nadler	X		
Mr. Scott			
Mr. Watt	X		
Ms. Lofgren	X		
Ms. Jackson Lee			
Ms. Waters			
Mr. Delahunt	X		
Mr. Wexler			
Mr. Cohen	X		
Mr. Johnson	X		
Mr. Pierluisi	X		

ROLLCALL NO. 10—Continued

	Ayes	Nays	Present
Mr. Quigley	X		
Ms. Chu	X		
Mr. Gutierrez	X		
Ms. Baldwin	X		
Mr. Gonzalez			
Mr. Weiner	X		
Mr. Schiff	X		
Ms. Sánchez			
Ms. Wasserman Schultz	X		
Mr. Maffei	X		
Mr. Smith, Ranking Member		X	
Mr. Sensenbrenner, Jr.			
Mr. Coble			
Mr. Gallegly		X	
Mr. Goodlatte		X	
Mr. Lungren		X	
Mr. Issa		X	
Mr. Forbes			
Mr. King			
Mr. Franks		X	
Mr. Gohmert			
Mr. Jordan		X	
Mr. Poe		X	
Mr. Chaffetz			
Mr. Rooney		X	
Mr. Harper		X	
Total	16	10	

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

NEW BUDGET AUTHORITY AND TAX EXPENDITURES

Clause 3(c)(2) of rule XIII of the Rules of the House of Representatives is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 3845, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, December 10, 2009.

Hon. JOHN CONYERS, Jr., *Chairman,*
Committee on the Judiciary,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3845, the USA PATRIOT Amendments 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, who can be reached at 226–2860.

Sincerely,

DOUGLAS W. ELMENDORF,
DIRECTOR.

Enclosure

cc: Honorable Lamar S. Smith.
Ranking Member

H.R. 3845—USA PATRIOT Amendments Act of 2009.

CBO estimates that implementing H.R. 3845 would cost about $9 million over the 2010–2014 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 H.R. 3845 are either excluded from review for mandates under the Unfunded Mandates Reform Act because they are necessary for national security or contain no mandates as defined by that act.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (Public Law 107–56) 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. H.R. 3845 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.

H.R. 3845 would require the DOJ Inspector General, by December 31, 2014, to conduct audits of the department's use of certain investigative powers during the 2007–2013 period. Based on information from DOJ, we expect that the department would need to hire about 10 people to carry out those audits. CBO estimates that auditing effort would cost about $1 million in fiscal year 2010, about $2 million annually over the 2011–2014 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 H.R. 3845 could be subject to civil and criminal fines, the Federal Government might collect additional fines if the legislation is enacted. Collec-

tions 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.

On October 23, 2009, CBO transmitted a cost estimate for S. 1692, the USA PATRIOT Act Sunset Extension Act of 2009, as reported by the Senate Committee on the Judiciary on October 13, 2009. That bill would require fewer DOJ audits and CBO estimated 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.

The CBO staff contact for this estimate is Mark Grabowicz. The estimate was approved by Theresa Gullo, Deputy Assistant Director for Budget Analysis.

PERFORMANCE GOALS AND OBJECTIVES

The Committee states that pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 3845 is intended to reauthorize and modify certain surveillance and information gathering authorities to ensure the government can conduct efficient, thorough and effective national security investigations, in a manner that appropriately protects privacy and civil liberties interests.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds the authority for this legislation in article I, section 8 of the Constitution.

ADVISORY ON EARMARKS

In accordance with clause 9 of rule XXI of the Rules of the House of Representatives, H.R. 3845 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(e), 9(f), or 9(g) of Rule XXI.

SECTION-BY-SECTION ANALYSIS

The following discussion describes the bill as reported by the Committee:

Sec. 1. Short title and table of contents. Section 1 sets forth the short title of the bill as the "USA PATRIOT Amendments Act of 2009" and provides a table of contents for the entire bill.

TITLE I—USA PATRIOT ACT RELATED AMENDMENTS

Sec. 101. Roving Wiretaps. Section 101 of the bill clarifies Congressional intent that when using roving wiretap authority, the government must describe its target with a sufficient degree of particularity to allow a judge to be able to distinguish the target from other potential users of places or facilities to be surveilled, so as to avoid surveillance of unrelated targets at unrelated places.

Sec. 102. Extension of Sunset of Sections 206 and 215 of USA PATRIOT Act. Section 102 of the bill extends the sunset dates of rov-

ing wiretaps and FISA business records provisions to December 31, 2013.

Sec. 103. Access to Certain Tangible Things under section 501 of the Foreign Intelligence Surveillance Act of 1978. Section 103 of the bill modifies the standard for obtaining a court order for tangible things under section 501 of FISA, as amended by section 215 of the USA PATRIOT Act, by removing the presumption of relevance for certain categories of documents, and requiring the government to provide a statement of facts and circumstances relied upon by the applicant to justify the applicant's belief that the tangible things sought are relevant to an authorized foreign intelligence, counterterrorism, or counterintelligence investigation. It permits a recipient to challenge both the underlying order and any associated nondisclosure order immediately, and requires the government to notify the recipient of this right at the time the order is served. It eliminates the government's right to conclusively defeat a challenge to a nondisclosure order with a certification. And it facilitates continuing court oversight of minimization procedures through compliance assessments pertaining to specific section 215 orders.

Section 103 of the bill also requires the government to meet a heightened standard for using a section 215 order to obtain personally identifiable information concerning library patrons and bookseller information, of "specific and articulable facts" showing that there are reasonable grounds to believe that the records sought are "relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities" *and* that the records "pertain to a foreign power or agent of a foreign power, are relevant to the activities of a suspected agent of a foreign power who is the subject of such authorized investigation, or pertain to an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation."

Sec. 104. Sunset Relating to Individual Terrorists as Agents of Foreign Powers. Section 104 of the bill allows the "Lone Wolf" provision to sunset on December 31, 2009.

Sec. 105. Audits. Section 105 of the bill requires the DOJ Inspector General to audit and submit reports to Congress for section 215 "tangible things" orders, national security letters (NSLs), and FISA pen register and trap-and-trace orders, and criminal pen register and trap-and-trace orders for all calendar years through 2013.

Sec. 106. Criminal "sneak and peek" searches. Section 106 of the bill shortens the period after which the government must seek an extension off time for delaying notice of a "sneak and peek" search warrant to seven (7) days, from the current 30 days or longer. Any single extension to delay notice granted by a court is limited to 21 days, though multiple extensions are possible. Moreover, any application for extension must be made by the Senate-confirmed United States Attorney for the district seeking the delay. If the government's rationale for delaying notice of the search is the possibility of jeopardizing an investigation or unduly delaying a trial, the government must now establish that such an outcome is "likely to" occur.

Sec. 107. Orders for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes. Section 107 of the bill modifies

the standard for obtaining a pen/trap to require the government to provide a statement of 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. Under current law, in order to obtain a FISA pen/trap, the government must merely certify that the information sought is foreign intelligence information or is relevant to an investigation to protect against international terrorism or clandestine intelligence activities.

Section 107 also codifies procedures for minimization of the retention and dissemination of information obtained pursuant to 50 U.S.C. § 1842, where appropriate in exceptional circumstances. This is intended to provide a statutory footing for the existing practice whereby specialized minimization procedures are implemented in certain limited circumstances, under FISC authorization and oversight.

Sec. 108. Public Reporting on the Foreign Intelligence Surveillance Act. Section 108 of the bill requires that annual public reporting of numbers of requests for surveillance be given separately for electronic surveillance, physical searches, tangible things orders, and pen registers, rather than the public reporting of these requests in one aggregate number.

Sec. 109. Challenges to Nationwide Orders for Electronic Surveillance. Section 109 of the bill permits a provider of electronic communications service or remote computing service to challenge a subpoena, order, or warrant requiring disclosure of customer communications or records in either the district in which the order was issued or the district in which the order was served. Current law only allows a challenge in the district where the order was issued.

Sec. 110. Report on Civil Liberties and Privacy Protections. Section 110 of the bill helps ensure that appropriate consideration is given to civil liberties protections with respect to 215 orders used to support sensitive collections, by calling on the President to report to Congress regarding whether such collections could be modified so as to enhance protections for civil liberties, the nature and likely costs of any potential modifications, and any technical challenges or potential impact on operations of potential modifications. This report is to be submitted to this Committee, the House Permanent Select Committee on Intelligence, and the Committee on the Judiciary and the Select Committee on Intelligence of the Senate, no later than 180 days after the date of enactment of the bill.

TITLE II—NATIONAL SECURITY LETTER REFORM

Sec. 201. Short Title. Section 201 sets forth the short tile of title II as the "National Security Letter Reform Act of 2009."

Sec. 202. Sunset. Section 202 provides a sunset date of December 31, 2013 for the new statutory authorization governing NSLs, after which the relevant NSL statutes would, in the absence of new legislation, revert to how they read on October 25, 2001, prior to enactment of the USA PATRIOT Act.

Sec. 203. National Security Letter Defined. Section 203 of the bill defines "national security letter," for the purposes of this bill, as a request for information under one of the enumerated provisions of law.

Sec. 204. Modification of Standard. Section 204 of the bill requires, before an NSL can issue, that an official with the authority to issue such letter document and retain a statement of specific and articulable facts showing that there are reasonable grounds to believe that the information sought: (1) pertains to a foreign power or an agent of a foreign power; (2) is relevant to the activities of a suspected agent of a foreign power that is the subject of such authorized investigation; or (3) pertains to an individual in contact with, or personally known to, a suspected agent of a foreign power that is the subject of such authorized investigation. Current law requires only relevance to an authorized investigation before an NSL can issue, and does not require a government official to document and retain a statement of facts showing how the new standard is satisfied.

Sec. 205. Notification of Right to Judicial Review of Nondisclosure Order. Section 205 of the bill requires the government to notify a recipient of an NSL of a right to judicial review of any nondisclosure requirement imposed in connection with the NSL, and provides that the nondisclosure requirement will remain in effect during the pendency of any judicial review proceedings. Current law does not require such notification.

Sec. 206. Disclosure for Law Enforcement Purposes. Section 206 of the bill requires the Attorney General, or a designee of the Attorney General at a level not lower than Section Chief of a division of the Department of Justice, to authorize the use of any information acquired from an NSL in a criminal proceeding. Current law does not impose any such authorization requirement.

Sec. 207. Judicial Review of National Security Letter Nondisclosure Order. Section 207 of the bill establishes additional procedures for a recipient to seek judicial review of a nondisclosure requirement imposed in connection with an NSL. These procedures correct Constitutional defects in the issuance of NSL nondisclosure orders identified by the Second Circuit in *Doe v. Mukasey.* If the recipient wishes to obtain court review of a nondisclosure requirement, the recipient must notify the government. The government has 30 days after the receipt of such notification to apply for a court order prohibiting disclosure regarding the NSL. The nondisclosure requirement remains in effect during the pendency of any judicial proceedings. The government's application for a nondisclosure order must include a certification from the Attorney General, the Deputy Attorney General, or the Director of the FBI (or the head of another agency if not part of DOJ) containing a statement of specific and articulable facts indicating that disclosure may result in a danger to the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or result in danger to the life or physical safety of a person. If a court determines that there is reason to believe that disclosure will result in one of the enumerated harms, the court may issue a nondisclosure order, for no longer than 180 days. The government can seek renewals of nondisclosure orders for additional periods of not longer than 180 days each. This section also eliminates the "conclusive certification" power under which certain high-level officials could make a general certification that disclosure might endanger the national security of the United States or interfere with diplomatic relations, with the

result that such certification or recertification would, unless made in bad faith, automatically defeat any challenge to a nondisclosure order.

Sec. 208. Minimization Procedures. Section 208 of the bill requires the Attorney General to establish minimization procedures governing the acquisition, retention, and dissemination by the Federal Bureau of Investigation in response to an NSL and to submit a copy of these procedures to this Committee, the House Permanent Select Committee on Intelligence, and the Committee on the Judiciary and the Select Committee on Intelligence of the Senate. Current statutory law does not require the government to apply minimization procedures to information acquired in response to an NSL, although this has become a common practice.

Sec. 209. Public Reporting on National Security Letters. Section 209 requires annual public reporting on the number of requests for NSLs and greater specificity of the types persons targeted (e.g., U.S. persons v. non-U.S. persons).

TITLE III—GENERAL PROVISIONS

Sec. 301. Sense of Congress on Level of Classification of Certain Programs. Section 301 of the bill expresses the sense of the Congress that the President should periodically review the level of classification of programs that make use of NSLs or authorities under the FISA statute, to determine if such programs can be declassified in whole or in part, without interfering with an ongoing investigation or otherwise threatening national security.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, existing law in which no change is proposed is shown in roman):

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Foreign Intelligence Surveillance Act of 1978".

TABLE OF CONTENTS

* * * * * * *

TITLE IV—PEN REGISTERS AND TRAP AND TRACE DEVICES FOR FOREIGN INTELLIGENCE PURPOSES

* * * * * * *

[TITLE V—ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE PURPOSES

[Sec. 501. Access to certain business records for foreign intelligence and international terrorism investigations.
[Sec. 502. Congressional oversight.]

* * * * * * *

TITLE I—ELECTRONIC SURVEILLANCE WITHIN THE UNITED STATES FOR FOREIGN INTELLIGENCE PURPOSES

* * * * * * *

ISSUANCE OF AN ORDER

SEC. 105. (a) * * *

* * * * * * *

(c)(1) * * *

(2) DIRECTIONS.—An order approving an electronic surveillance under this section shall direct—

(A) * * *

(B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person, or in circumstances where the Court [finds, based upon specific facts] *finds—*

(i) that the target of the application is a foreign power, as defined in paragraph (1), (2), (3), or (6) of section 101(a), an agent of such a foreign power, or a specific individual; and

(ii) based upon specific facts provided in the application, that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons, furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

* * * * * * *

TITLE IV—PEN REGISTERS AND TRAP AND TRACE DEVICES FOR FOREIGN INTELLIGENCE PURPOSES

DEFINITIONS

SEC. 401. As used in this title:

(1) * * *

* * * * * * *

(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.

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

SEC. 402. (a) * * *

* * * * * * *

(c) 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 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 proposed minimization procedures.

(d)(1) * * *

(2) An order issued under this section—

(A) * * *

* * * * * * *

(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) * * *

* * * * * * *

(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) * * *

* * * * * * *

(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[.]*; and*

(D) shall, if the judge finds that there are exceptional circumstances, direct that minimization procedures be followed.

* * * * * * *

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

AUTHORIZATION DURING EMERGENCIES

SEC. 403. (a) * * *

* * * * * * *

(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.

[(c)] *(d)*(1) * * *

* * * * * * *

USE OF INFORMATION

SEC. 405. (a)(1) Information acquired from the use of a pen register or trap and trace device installed pursuant to this title 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 *and the minimization procedures under this title, if required*.

* * * * * * *

TITLE V—ACCESS TO [CERTAIN BUSINESS RECORDS] *TANGIBLE THINGS* FOR FOREIGN INTELLIGENCE PURPOSES

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

(a) * * *

(b) Each application under this section—

(1) * * *

(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) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or [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] *clandestine intelligence activities;*

(B) if the records sought contain bookseller information, or are from a library (as defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1))) and contain personally identifiable information about a patron of such library, a statement of specific and articulable 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 who is the subject of such authorized investigation; and

[(B)] *(C)* an enumeration of the minimization procedures adopted by the Attorney General under subsection (g) 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.

(c)(1) * * *

(2) An order under this subsection—

(A) * * *

* * * * * * *

(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] *things;*

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

(F) shall direct the applicant to provide notice to each person receiving such order of—

(i) the right to challenge the legality of a production order or nondisclosure order by filing a petition in accordance with subsection (f); and

(ii) the procedures to follow to file such petition in accordance with such subsection.

* * * * * * *

(f)(1) * * *

(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 103(e)(1). [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 103(e)(1).]

(ii) The presiding judge shall immediately assign a petition under clause (i) to 1 of the judges serving in the pool established by section 103(e)(1). Not later than 72 hours after the assignment of such petition, the assigned judge shall conduct an initial review of the petition. If the assigned judge determines that the petition is frivolous, the assigned judge shall immediately deny the petition and affirm the [production order or nondisclosure] order. If the assigned judge determines the petition is not frivolous, the assigned judge shall promptly consider the petition in accordance with the procedures established under section 103(e)(2).

* * * * * * *

(C)(i) * * *

[(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.]

[(iii)] *(ii)* 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.

* * * * * * *

(g) MINIMIZATION PROCEDURES.—

(1) * * *

(2) COMPLIANCE ASSESSMENT.—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 such order, a judge may assess compliance with the minimization procedures required to be followed under such order by reviewing the circumstances under

which information concerning United States persons was retained or disseminated.

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

(A) * * *

* * * * * * *

(i) BOOKSELLER INFORMATION DEFINED.—In this section, the term "bookseller information" means personally identifiable information concerning the purchase (including subscription purchases) or rental of books, journals, or magazines, whether in print or digitally.

* * * * * * *

TITLE VI—REPORTING REQUIREMENT

SEC. 601. SEMIANNUAL REPORT OF THE ATTORNEY GENERAL.

(a) * * *

(b) PUBLIC REPORT.—The Attorney General shall make publicly available the portion of each report under subsection (a) relating to paragraph (1) of such subsection.

[(b)] *(c)* FREQUENCY.—The first report under this section shall be submitted not later than 6 months after the date of enactment of this section. Subsequent reports under this section shall be submitted semi-annually thereafter.

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

(1) * * *

* * * * * * *

[(d)] *(e)* PROTECTION OF NATIONAL SECURITY.—The Attorney General, in consultation with the Director of National Intelligence, may authorize redactions of materials described in [subsection (c)] *subsection (d)* that are provided to the committees of Congress referred to in subsection (a), if such redactions are necessary to protect the national security of the United States and are limited to sensitive sources and methods information or the identities of targets.

[(e)] *(f)* DEFINITIONS.—In this section:

(1) * * *

* * * * * * *

USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT OF 2005

* * * * * * *

TITLE I—USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT

* * * * * * *

SEC. 102. USA PATRIOT ACT SUNSET PROVISIONS.

(a) * * *

(b) SECTIONS 206 AND 215 SUNSET.—

(1) IN GENERAL.—Effective [December 31, 2009] *December 31, 2013*, the Foreign Intelligence Surveillance Act of 1978 is amended so that sections 501, 502, and 105(c)(2) read as they read on October 25, 2001.

* * * * * * *

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

(a) * * *

(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 [2006] *2013*, including—

(A) * * *

* * * * * * *

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

(A) * * *

* * * * * * *

(C) with respect to [calendar year 2006] *each of calendar years 2006 through 2013*, an examination of the minimization procedures adopted by the Attorney General under section 501(g) of such Act and whether such minimization procedures protect the constitutional rights of United States persons;

* * * * * * *

(c) SUBMISSION DATES.—

(1) * * *

* * * * * * *

(3) CALENDAR YEARS 2007 THROUGH 2009.—Not later than December 31, 2010, 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 through 2009.

(4) CALENDAR YEARS 2010 THROUGH 2013.—Not later than December 31, 2011, and annually thereafter until December 31, 2014, 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 the preceding calendar year.

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

(1) NOTICE.—Not less than 30 days before the submission of a report under subsection (c)(1) [or (c)(2)], *(c)(2), (c)(3), or (c)(4)*, 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) [and (c)(2)], *(c)(2), (c)(3), or (c)(4)* as the Attorney General or the Director of National Intelligence may consider necessary.

(e) UNCLASSIFIED FORM.—The reports submitted under subsections (c)(1) [and (c)(2)], *(c)(2), (c)(3), or (c)(4)* 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.

(a) * * *

* * * * * * *

(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];

* * * * * * *

(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).

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

* * * * * * *

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

(a) * * *

(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 [2006] *2013*;

* * * * * * *

(c) SUBMISSION DATES.—

(1) * * *

* * * * * * *

(3) CALENDAR YEARS 2007 THROUGH 2009.—Not later than December 31, 2010, 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 through 2009.

(4) CALENDAR YEARS 2010 THROUGH 2013.—Not later than December 31, 2011, and annually thereafter until December 31, 2014, 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 the previous calendar year.

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

(1) NOTICE.—Not less than 30 days before the submission of a report under subsection (c)(1) [or (c)(2)], *(c)(2), (c)(3), or (c)(4)*, 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) [or (c)(2)], *(c)(2), (c)(3), or (c)(4)* as the Attorney General or the Director of National Intelligence may consider necessary.

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

* * * * * * *

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004

* * * * * * *

TITLE VI—TERRORISM PREVENTION

Subtitle A—Individual Terrorists as Agents of Foreign Powers

SEC. 6001. INDIVIDUAL TERRORISTS AS AGENTS OF FOREIGN POWERS.

(a) * * *

(b) SUNSET.—

(1) IN GENERAL.—Except as provided in paragraph (2), [the amendment made by subsection (a) shall cease to have effect] *effective* on December 31, 2009[.]—

(A) subparagraph (C) of section 101(b)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(b)(1)) is repealed;

(B) subparagraphs (D) and (E) of such section are redesignated as subparagraphs (C) and (D), respectively;

(C) paragraph (2) of section 601(a) of such Act (50 U.S.C. 1871(a)) is repealed; and

(D) paragraphs (3), (4), and (5) of such section are redesignated as paragraphs (2), (3), and (4), respectively.

(2) [EXCEPTION] *EXCEPTION.—*

(A) EXISTING INVESTIGATIONS.—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 the provisions cease to have effect, such provisions shall continue in effect.

(B) REPORTS.—Notwithstanding the repeals made by paragraph (1), the first report required under section 601(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1871(a)) that is submitted after the effective date of such repeals shall include the number of individuals covered by an order issued pursuant to section 101(b)(1)(C) of such Act (as in effect on the day before such effective date).

* * * * * * *

TITLE 18, UNITED STATES CODE

* * * * * * *

PART I—CRIMES

* * * * * * *

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

* * * * * * *

§ 2703. Required disclosure of customer communications or records

(a) * * *

* * * * * * *

(h) JUDICIAL REVIEW.—A provider of electronic communication service or remote computing service may challenge a subpoena, order, or warrant requiring disclosure of customer communications or records under this section in—

(1) the United States district court for the district in which the order was issued; or

(2) the United States district court for the district in which the order was served.

* * * * * * *

[Pursuant to section 202(a) of H.R. 3845, effective December 31, 2013, section 2709 is amended to read as such section read on October 25, 2001.]

[§ 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).

[(d) DISSEMINATION BY BUREAU.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

[(e) REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES BE INFORMED.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

[(f) LIBRARIES.—A library (as that term is defined in section 213(1) of the Library Services and Technology Act (20 U.S.C. 9122(1)), the services of which include access to the Internet, books, journals, magazines, newspapers, or other similar forms of commu-

nication 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.]

§ 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, may—

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

(A) the name, address, length of service, and toll billing records sought are relevant to an authorized foreign counterintelligence investigation; and

(B) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801); and

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

(A) the information sought is relevant to an authorized foreign counterintelligence investigation; and

(B) there are specific and articulable facts giving reason to believe that communication facilities registered in the name of the person or entity have been used, through the services of such provider, in communication with—

(i) an individual who is engaging or has engaged in international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States; or

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

(c) PROHIBITION OF CERTAIN DISCLOSURE.— No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) DISSEMINATION BY BUREAU.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES BE INFORMED.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under subsection (b) of this section.

* * * * * * *

PART II—CRIMINAL PROCEDURE

* * * * * * *

CHAPTER 205—SEARCHES AND SEIZURES

* * * * * * *

§ 3103a. Additional grounds for issuing warrant

(a) * * *

(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)**]** *may endanger the life or physical safety of an individual, result in flight from prosecution, result in the destruction of or tampering with the evidence sought under the warrant, or result in intimidation of potential witnesses, or is likely to otherwise seriously jeopardize an investigation or unduly delay a trial*;

* * * * * * *

(3) the warrant provides for the giving of such notice within a reasonable period not to exceed **[**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.] *7 days after the date of its execution.*

(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.] *upon application of the United States Attorney for the district seeking the delay, for additional periods of not more than 21 days for each application, if the court finds, for each application, reasonable cause to believe that notice of the execution of the warrant may endanger the life or physical safety of an individual, result in flight from prosecution, result in the destruction of or tampering with the evidence sought under the warrant, or result in intimidation of potential witnesses, or is likely to otherwise seriously jeopardize an investigation or unduly delay a trial.*

* * * * * * *

CHAPTER 223—WITNESSES AND EVIDENCE

* * * * * * *

§ 3511. Judicial review of requests for information

(a) * * *

[(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 Report-

ing 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 (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, 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 particular information about 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 may issue a nondisclosure order for a period of not longer than 180 days.

(D) DENIAL.—If a district court of the United States rejects an application for a nondisclosure order or extension thereof, the nondisclosure requirement shall no longer be in effect.

(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, of the existence of a result described in subparagraphs (A) through (D) and 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 may issue a nondisclosure requirement order or extension thereof under this subsection if the court determines that there is reason to believe that disclosure of the information subject to the nondisclosure requirement during the applicable time period will have a result described in paragraph (2).

(4) RENEWAL.—A nondisclosure order under this subsection may be renewed for additional periods of not longer than 180 days each, upon a determination by the court that a result described in paragraph (2) justifies the renewal.

(5) EARLY TERMINATION OF NONDISCLOSURE ORDER.—A nondisclosure order the Government applied for under paragraph (1)(B) ceases to have effect when the Government discovers that the factual basis for that order has ceased to exist and the Government so informs the order's recipient. The Government upon making such a discovery shall promptly so informs the recipient.

* * * * * * *

SECTION 1114 OF THE RIGHT TO FINANCIAL PRIVACY ACT OF 1978

[Pursuant to section 202(a) of H.R. 3845, effective December 31, 2013, section 1114(a)(5) is amended to read as such paragraph read on October 25, 2001.]

SPECIAL PROCEDURES

SEC. 1114. (a)(1) * * *

* * * * * * *

[(5)(A) Financial institutions, and officers, employees, and agents thereof, shall comply with a request for a customer's or entity's financial records made pursuant to this subsection by the Federal Bureau of Investigation when the Director of the Federal Bureau of Investigation (or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director) certifies in writing to the financial institution that such records are sought for foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

[(B) The Federal Bureau of Investigation may disseminate information obtained pursuant to this paragraph only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

[(C) On the dates provided in section 507 of the National Security Act of 1947, the Attorney General shall fully inform the congressional intelligence committees (as defined in section 3 of that Act (50 U.S.C. 401a)) 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).]

(5)(A) Financial institutions, and officers, employees, and agents thereof, shall comply with a request for a customer's or entity's financial records made pursuant to this subsection by the Federal Bureau of Investigation when the Director of the Federal Bureau of Investigation (or the Director's designee) certifies in writing to the financial institution that such records are sought for foreign counterintelligence purposes and that there are specific and articulable facts giving reason to believe that the customer or entity whose records are sought is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(B) The Federal Bureau of Investigation may disseminate information obtained pursuant to this paragraph only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(C) On a semiannual basis the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made pursuant to this paragraph.

(D) No financial institution, or officer, employee, or agent of such institution, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to a customer's or entity's financial records under this paragraph.

* * * * * * *

TITLE VI—CONSUMER CREDIT REPORTING

* * * * * * *

§ 601. Short title

This title may be cited as the "Fair Credit Reporting Act".

* * * * * * *

[Pursuant to section 202(a) of H.R. 3845, effective December 31, 2013, sections 626(a), 626(b), and 627 are amended to read as such sections read on October 25, 2001.]

§ 626. Disclosures to FBI for counterintelligence purposes

[(a) IDENTITY OF FINANCIAL INSTITUTIONS.—Notwithstanding section 604 or any other provision of this title, a consumer reporting agency shall furnish to the Federal Bureau of Investigation the names and addresses of all financial institutions (as that term is defined in section 1101 of the Right to Financial Privacy Act of 1978) at which a consumer maintains or has maintained an account, to the extent that information is in the files of the agency, when presented with a written request for that information, signed by the Director of the Federal Bureau of Investigation, or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director, which certifies compliance with this section. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing, that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

[(b) IDENTIFYING INFORMATION.—Notwithstanding the provisions of section 604 or any other provision of this title, a consumer reporting agency shall furnish identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a written request, signed by the Director or the Director's designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge of a Bureau field office designated by the Director, which certifies compliance with this subsection. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that such information is sought for the conduct of an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of ac-

tivities protected by the first amendment to the Constitution of the United States.]

(a) IDENTITY OF FINANCIAL INSTITUTIONS.—Notwithstanding section 604 or any other provision of this title, a consumer reporting agency shall furnish to the Federal Bureau of Investigation the names and addresses of all financial institutions (as that term is defined in section 1101 of the Right to Financial Privacy Act of 1978) at which a consumer maintains or has maintained an account, to the extent that information is in the files of the agency, when presented with a written request for that information, signed by the Director of the Federal Bureau of Investigation, or the Director's designee, which certifies compliance with this section. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that—

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

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

(A) is a foreign power (as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978) or a person who is not a United States person (as defined in such section 101) and is an official of a foreign power; or

(B) is an agent of a foreign power and is engaging or has engaged in an act of international terrorism (as that term is defined in section 101(c) of the Foreign Intelligence Surveillance Act of 1978) or clandestine intelligence activities that involve or may involve a violation of criminal statutes of the United States.

(b) IDENTIFYING INFORMATION.—Notwithstanding the provisions of section 604 or any other provision of this title, a consumer reporting agency shall furnish identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment, to the Federal Bureau of Investigation when presented with a written request, signed by the Director or the Director's designee, which certifies compliance with this subsection. The Director or the Director's designee may make such a certification only if the Director or the Director's designee has determined in writing that—

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

(2) there is information giving reason to believe that the consumer has been, or is about to be, in contact with a foreign power or an agent of a foreign power (as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978).

* * * * * * *

[§ 627. Disclosures to governmental agencies for counterterrorism purposes

[(a) DISCLOSURE.—Notwithstanding section 604 or any other provision of this title, 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 writ-

ten certification by such government agency that such information is necessary for the agency's conduct or such investigation, activity or analysis.

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

[(c) CONFIDENTIALITY.—

[(1) If the head of a government agency authorized to conduct investigations of intelligence or counterintelligence activities or analysis related to international terrorism, or his designee, certifies that otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person, no consumer reporting agency or officer, employee, or agent of such consumer reporting agency, shall disclose to any person (other than those to whom such disclosure is necessary to comply with the request or an attorney to obtain legal advice or legal assistance with respect to the request), or specify in any consumer report, that a government agency has sought or obtained access to information under subsection (a).

[(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).

[(d) RULE OF CONSTRUCTION.—Nothing in section 626 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 title, any consumer reporting agency or agent or employee thereof making disclosure of consumer reports or other information pursuant to this section in good-faith reliance upon a certification of a government agency pursuant to the provisions of this section shall not be liable to any person for such disclosure under this subchapter, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

[(f) REPORTS TO CONGRESS.—(1) On a semi-annual basis, the Attorney General shall fully inform the Committee on the Judiciary, the Committee on Financial Services, and the Permanent Select Committee on Intelligence of the House of Representatives and the Committee on the Judiciary, the Committee on Banking, Housing, and Urban Affairs, and the Select Committee on Intelligence of the Senate concerning all requests made pursuant to subsection (a).

[(2) In the case of the semiannual reports required to be submitted under paragraph (1) to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, the submittal dates for such reports shall be as provided in section 507 of the National Security Act of 1947 (50 U.S.C. 415b).]

* * * * * * *

SECTION 802 OF THE NATIONAL SECURITY ACT OF 1947

[Pursuant to section 202(a) of H.R. 3845, effective December 31, 2013, section 802 is amended to read as such section read on October 25, 2001.]

[REQUESTS BY AUTHORIZED INVESTIGATIVE AGENCIES

[SEC. 802. (a)(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).

[(b) PROHIBITION OF CERTAIN DISCLOSURE.—

[(1) If an authorized investigative agency described in subsection (a) 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).

[(c)(1) Notwithstanding any other provision of law (other than section 6103 of the Internal Revenue Code of 1986), an entity receiving a request for records or information under subsection (a) 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 title, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

[(d) 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) 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) 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.).]

REQUESTS BY AUTHORIZED INVESTIGATIVE AGENCIES

SEC. 802. (a)(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 in-

formation 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).

(b) Notwithstanding any other provision of law, no governmental or private entity, or officer, employee, or agent of such entity, may disclose to any person, other than those officers, employees, or agents of such entity necessary to satisfy a request made under this section, that such entity has received or satisfied a request made by an authorized investigative agency under this section.

(c)(1) Notwithstanding any other provision of law (other than section 6103 of the Internal Revenue Code of 1986), an entity receiving a request for records or information under subsection (a) 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 title, the constitution of any State, or any law or regulation of any State or any political subdivision of any State.

(d) 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) 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) 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.).

DISSENTING VIEWS

We oppose H.R. 3845, which unnecessarily weakens America's counter-terrorism laws and impairs our intelligence-gathering capabilities. This legislation is nothing more than change for the sake of change. The majority has seen fit to defy the Obama Administration's call for full reauthorization of the Act's expiring provisions and instead placate extreme liberal interest groups that have decried the very existence of the USA PATRIOT Act since its enactment in 2001.

To be sure, the majority espouses reforms to our foreign intelligence or criminal laws, claiming such reforms are needed to prevent the abuse or misuse of these laws. Such claims are hollow and without merit. Not only has the majority failed to provide evidence of the government's misuse or abuse of many of these provisions, they offer no explanation for how their proposed reforms will correct any such supposed misuse. It is apparent that they are not even certain how their legislation will affect the use of these laws.

With every "change for the sake of change" this bill makes, the majority threatens the ongoing and critical collection of foreign intelligence and risks empowering radical jihadists, terrorists, and spies to ramp up their efforts to attack the United States. This legislation also signals to the courts that Congress urges a different interpretation of these provisions, but with little to no guidance as to what ill Congress seeks to cure. This is a dangerous risk to take with our foreign intelligence laws—laws that should only be amended when absolutely necessary.

TITLE I—USA PATRIOT ACT RELATED AMENDMENTS

Roving Wiretaps

Section 101, as introduced, requires the government to include additional information in applications to the Foreign Intelligence

Surveillance Court ("FISC")for orders that authorize wiretap surveillance of a foreign intelligence target. In cases where the identity of the target of the surveillance order is unknown, the government must provide additional information "sufficient to allow a judge to determine that the target is a single individual."

Liberal interest groups have taken issue with so-called "John Doe" surveillance orders. In testimony before the Constitution Subcommittee, the ACLU wrote that the authority gave law enforcement officials "an inappropriate level of discretion" because it "does not require the government to name the target, or to make sure its roving wiretaps are intercepting only the target's communications." The ACLU further argues that roving wiretaps should have the same fourth amendment warrant requirements as Title III criminal wiretaps.

This assertion fails to acknowledge the key differences between the two investigative tools. Title III wiretaps are used to investigate Federal crimes, while Foreign Intelligence Surveillance Act ("FISA") wiretaps are used in national security and foreign intelligence investigations. Moreover, the wiretaps rely on two different probable cause standards (e.g., with FISC court orders, the "probable cause" showing is not of criminal activity, but of a connection between that target and a "foreign power").

We note that the provision, as introduced, does not go as far as to align the requirements of FISC court orders with those of Title III (criminal) wiretaps, but the language will require law enforcement officials to clear a higher evidentiary bar than that of current law. This new language is troublesome as it adds, for no demonstrated reason, additional burdens to the already substantial list of requirements for obtaining a FISC court order for these important tools.

The manager's amendment offered by Chairman Conyers corrects what we can only presume was a significant drafting error in the roving wiretap provision. In an attempt to address the misperceived "John Doe" roving wiretap, the underlying bill actually limits all FISA surveillance to a single individual target. This is unworkable because FISA authorizes, among other things, the surveillance of "foreign powers," which presumably involve much more than a single individual.

The manager's amendment applies this limitation just to the roving wiretap provision and not all electronic surveillance. But even this language attempts to solve a problem that does not exist and for which no factual record has been developed. As with so many provisions in this bill, the change to the roving wiretap provision is change for the sake of change.

FISA Business Records

Standard

Section 103, as introduced, reverts back to the pre-9/11 standard of "specific and articulable facts," which proved cumbersome for the intelligence community's use of this and other provisions with the same standard. Current law already imposes significant requirements on the government in its applications for business records in national security and terrorism cases. The government must submit a statement of facts showing reasonable grounds to believe that

the business records sought are relevant to an authorized investigation.

More importantly, we know that business records authority has been used to support important and highly sensitive intelligence collection operations. And we also know that by returning to a specific and articulable standard, we risk terminating or significantly curtailing these operations.

Increasing the standard to require "specific and articulable facts" will not, as the majority asserts, provide additional civil liberties protections to Americans. Current law already protects the free speech rights of Americans by preventing the use of this authority solely on the basis of activities protected by the first amendment. Such a standard will, however, provide greater protection to terrorists or spies by limiting the government's use of this authority.

We are pleased that Mr. Schiff offered an amendment to remove the specific and articulable facts standard and we supported this improvement to the bill. However, Mr. Schiff's amendment went further to delete a provision in current law instructing that business records sought by the government are presumptively relevant if the government shows that the records sought pertain to: (a) a foreign power or an agency 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.

Although we appreciate Mr. Schiff's intent to reach a compromise for the business records standard, his amendment sought to remove a provision without a full understanding of the consequences. We received no testimony or other evidence that the presumption of relevance is the source of any malfeasance with business records orders. Nor are we aware of how removing this presumption corrects any perceived misuse of these court orders. And we know that the affected Executive Branch agencies did not have an opportunity to weigh in on this important question.

For these reasons, Mr. Lungren offered a second-degree amendment to maintain the current presumption of relevance. We indicated to the majority that if they accepted Mr. Lungren's amendment, we would support Mr. Schiff's amendment. The majority declined and opposed Mr. Lungren's amendment. Therefore, despite our support for removing the specific and articulable facts standard, we were forced to oppose Mr. Schiff's amendment due the unnecessary and unjustified removal of the presumption of relevance.

Library and Bookseller Records

As introduced, section 103 exempts library patron lists and book customer lists from the universe of "tangible things" for which a business record order may be sought. The bill also prohibits any application for records of "a bookseller or library documentary materials that contain personally identifiable information concerning a patron of a bookseller or library."

The bill broadly defines "bookseller" as "any person or entity engaged in the sale, rental or delivery of books, journals, magazines, or other similar forms of communication in print or digitally." The bill also broadly defines the terms "personally identifiable information" and "documentary materials."

This prohibition is completely unnecessary and creates a safe-haven for terrorists to utilize America's libraries, bookstores, and websites to research and study bomb-making or other dangerous topics.

The manager's amendment replaces this outright prohibition with the heightened standard of "specific and articulable facts" for library and bookseller records. This change, however, is still unacceptable.

The 2005 USA PATRIOT Act reauthorization provided heightened protections for library and bookstore business records. Applications for orders seeking library circulation records, library patron lists, book sales records, and book customer lists may only be approved by the Director of the Federal Bureau of Investigation, the Deputy Director of the Federal Bureau of Investigation, or the Executive Assistant Director for National Security. And this authority cannot be further delegated. And business records orders—which are issued by the FISC—can only be accessed as part of a foreign intelligence, international terrorism, or clandestine intelligence investigation.

Moreover, as noted above, the business records provision currently protects the free speech rights of Americans by preventing the use of this authority solely on the basis of activities protected by the first amendment. The majority continues to operate under the misguided notion that library and bookseller records are of particular interest to Federal investigators. There is simply no evidence to support this belief and therefore no justification for imposing a heightened standard for library or bookseller records.

Mr. Gallegly offered an amendment to strike the portion of the manager's amendment that creates a heightened standard for library and bookseller business records, which the majority rejected.

Conclusive Treatment

Section 103 also eliminates the current requirement that the FISC treat as conclusive the government's certification that disclosure may endanger the national security of the United States or interfere with diplomatic relations, unless the court finds that such certification was made in bad faith.

By striking the conclusive treatment provision, the majority is instructing the FISC to afford no weight to the government's certification. This, despite the fact that Federal courts have long recognized that the President and the Executive Branch, as the experts on national security and foreign intelligence information, must be afforded deference in their determinations that the disclosure of certain information may endanger America.

"[C]ourts traditionally have been reluctant to intrude upon the authority of the Executive in . . . national security affairs,"[1] and the Supreme Court has acknowledged that terrorism may provide the basis for arguments "for heightened deference to the judgments of the political branches with respect to matters of national security."[2]

Last December, the Second Circuit Court of Appeals issued a decision in *Doe v. Mukasey*[3] relating to the nondisclosure provision

[1] *Department of Navy v. Egan,* 484 U.S. 518, 530 (1988).
[2] *Zadvydas v. Davis,* 533 U.S. 678, 696 (2001).
[3] 549 F.3d 861 (2nd Cir. 2008)

of certain National Security Letters. Like business records, National Security Letters afford conclusive treatment of the government's certification that disclosure may endanger the national security of the United States or interfere with diplomatic relations.

In *Doe*, the court held this conclusive treatment of NSL non-disclosure unconstitutional as inconsistent with strict scrutiny standards for a content-based prior restraint on first amendment protected speech. However, the court did not find that in the absence of conclusive treatment, there should be no weight afforded the government's certification.

On the contrary, the court continued to acknowledge the precedents that a level of deference must still be afforded the Executive Branch's assessment of dangers posed to national security by disclosure of a National Security Letter.[4] The same holds true for business records orders.

For this reason, Mr. Lungren offered an amendment to instruct the FISC to afford "substantial weight" to the government's certification. Despite the substantial number of long-standing precedents requiring courts to provide deference to the Executive Branch on national security matters, we were concerned that the FISC would interpret the removal of conclusive treatment with no standard in its stead as Congress' intent that no deference be afforded the government for the purposes of business record non-disclosure.

The Supreme Court has repeatedly afforded even greater deference than the "substantial weight" called for in Mr. Lungren's amendment. "The Court also has recognized 'the generally accepted view that foreign policy was the province and responsibility of the Executive. As to these areas of Article II duties the courts have traditionally shown the utmost deference to Presidential responsibilities.'"[5]

Despite this well-established rule, the majority opposed Mr. Lungren's amendment—a potential signal to the FISC that Congress intends no deference whatsoever even though Executive Branch officials are entitled to deference because they have awareness of the full scope of intelligence and investigative information concerning the matter for which the information is sought.

Sunset of Lone Wolf

Section 104 of the bill repeals the so-called "lone wolf" provision, which is set to expire on December 31, 2009. Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) amended the definition of "agent of a foreign power" in FISA (50 U.S.C. § 1801(b)) to include the "lone wolf" definition. This definition allows the government to surveil a non-U.S. person who is engaging in international terrorism or activities in preparation of international terrorism even if that target is not a foreign power or an agent of a foreign power.

FISA was originally enacted in 1978 to address surveillance of "foreign powers" and "agents of a foreign power." In 1978, America was in the midst of the Cold War, and Congress' primary concern was authorizing the surveillance of foreign powers, such as the Soviet Union, and their agents.

---

[4] *Id.* at 881.
[5] *Egan,* 484 U.S. at 529–30 (citations omitted).

Congress modernized FISA in 2004 to apply to a lone-wolf terrorist following the terrorist attacks of 9/11 faced with the stark reality that our enemies had changed. No longer were we concerned simply with foreign governments, but also with illusive and often anonymous terrorists spread throughout the world who may not fit the definition of "agent of a foreign power" as written in 1978.

To date, the government has never acknowledged use of this provision. The majority relies upon this as justification to let the provision expire. These authorities were enacted after 9/11 to fill gaps in the law. The fact that this particular gap was closed may have deterred a lone terrorist from attacking within this country since the provision was enacted.

It would be short-sighted to limit the government's ability to monitor an individual foreign terrorist who is working alone within the United States. It is not so hard to imagine a terrorist who might break away from al-Qaeda for ideological reasons and set out to commit terrorist acts on their own.

There is no reason why our intelligence gathering tools should not be used against terrorists seeking to attack our country simply because they are not known to be affiliated with a terrorist organization. It makes no sense to allow these individual terrorists who seek to kill Americans to slip through the cracks simply because they are not outwardly associated with al-Qaeda or another terrorist organization.

Ranking Member Smith offered an amendment to strike the repeal of section 6001 and extend the sunset of the lone wolf provision to December 31, 2013. This amendment failed on a tie vote.

In rejecting Mr. Smith's amendment, the majority argued that the government can use Title III criminal wiretaps to monitor terrorists. However, criminal wiretaps are ill-suited for use in intelligence operations. First, once criminal proceedings are instigated, the sixth amendment provides a criminal defendant with the right to a public trial, to be confronted with the witnesses against him, and to present relevant evidence in his defense.[6] In some prosecutions, particularly terrorism and espionage prosecutions, the defendant's presentation of evidence in a public trial may risk the national security of the United States.

Moreover, FISA wiretaps are used to collect foreign intelligence information that is highly classified, generally used for purposes other than a criminal trial, and not intended to be given to the target. Further, FISA protects the sources and methods of the government surveillance; this is information that criminal wiretaps do not protect. Gathering intelligence through the use of a criminal wiretap could tip off the terrorists to the strategies we use to track terrorists and intercept them before they strike.

The majority contends that all of these concerns are addressed by the Classified Information Procedures Act (CIPA).[7] CIPA "provides pretrial procedures that will permit the trial judge to rule on questions of admissibility involving classified information before introduction of the evidence in open court."[8] These procedures are in-

[6] U.S. Const. amend VI.
[7] P.L. 96–456, *codified at* 18 U.S.C. app. 3 § 1–16.
[8] S. REPT. 96–823, at 1.

tended to provide a means for the court to determine whether classified information is actually material to the defense.

Despite the majority's contention, CIPA is an inadequate alternative to FISA. First, foreign intelligence surveillance orders are approved by the FISC, which is comprised of 11 Federal district judges with an expertise in and extensive knowledge of the government's intelligence-collection operations. It was Congress' prerogative when it adopted FISA in 1978 that this subset of Federal judges be designated by the Chief Justice to serve on the FISC. Now the majority seeks to depart from Congress' intent and open-up the approval of these highly-sensitive orders to any and all Federal district court judges for lone terrorist investigations.

Second, CIPA is relevant only once criminal charges have been brought against a defendant. It is intended to provide uniform procedures for determining the admissibility of evidence on a case-by-case basis. This creates two uncertainties: (1) whether foreign intelligence information collected against a lone terrorist remain secure in the interim between collection and the commencement of criminal proceedings, if any; and (2) whether CIPA will be appropriately applied in each instance to protect the disclosure of classified information.

Although CIPA is useful for protecting classified information once a criminal proceeding has commenced, it and Title III wiretaps are a poor substitute to foreign intelligence collection under FISA.

Criminal wiretaps also require "live minimization" to ensure that the government does not gather evidence on protected activities. Live minimization is nearly impossible in foreign intelligence collection because most of the information captured by FISA wiretaps is in a foreign language. It is recorded live, but later translated by linguists at intelligence agencies. Under the Title III process, it would be nearly impossible for the government to engage in "live minimization" of predominantly foreign language information.

Delayed-Notice Search Warrants

Current law codifies the court's ability to delay the notice to the target of a search if it finds that notice "may" have an adverse result. Under 18 U.S.C. § 3103a, notice of a search warrant *may* be delayed if the issuing court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have the adverse result of (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; or (4) intimidation of potential witnesses.[9] In some circumstances, the statute further allows the court to delay notification if such notification would seriously jeopardize an investigation or unduly delay a trial.

Section 106 of this bill changes the standard for delayed notice from "may" to "will" have an adverse result. This change begs the question of how a court could ever determine that an adverse result "will" result unless notification is already delayed. The answer is it won't. Although Federal judges are very able and intelligent, they do not have the ability to accurately foresee the future. This legislation ignores that reality and would require the court to make

[9] 18 U.S.C. §§ 3103a(b)(1); 2705(a)(2).

a conclusive finding about the future. This requirement is based on an unattainable standard that will cripple the use of a decades-old, constitutional authority.

In 1979, the U.S. Supreme Court expressly held in *Dalia v. United States* that the fourth amendment does not require law enforcement to give immediate notice of the execution of a search warrant.[10] Three Federal courts of appeals had considered the constitutionality of delayed-notice search warrants since 1979 and upheld their constitutionality.[11] The USA PATRIOT Act codified the process for use of delayed notice search warrants, ensuring that notice may not be delayed indefinitely. The proposed changes in this bill revise these provisions to make them unduly burdensome to the government and the court.

As introduced, section 106 also eliminates the court's ability to delay notification if such notification would seriously jeopardize an investigation or unduly delay a trial. Of particular concern is the "seriously jeopardizing an investigation" justification. Federal agents investigating a terrorism case may have grounds to conduct a search of a suspect's home, office, storage unit, or other place, but not be prepared to bring an indictment or arrest the suspect.

It is also very likely that there is no evidence to suggest that this suspect will (1) endanger the life or physical safety of an individual, (2) flee from prosecution, (3) destroy or tamper with evidence, or (4) intimidate a witness. But that doesn't mean that we want to alert a terrorist to the fact that he is being investigated. Eliminating the "seriously jeopardizing an investigation" as a reason for delaying notification could force law enforcement agents to alert a terrorist to the fact that he is the subject of an investigation.

Mr. Issa offered an amendment to strike section 106. The majority sought an opportunity to discuss a compromise with Mr. Issa, and he withdrew his amendment. Mr. Issa offered a second amendment to reinstate the "may" standard and authorize the court to approve of delayed notice if the court finds that such a delay "is likely to" seriously jeopardize an investigation or unduly delay a trial. While this is a significant step towards maintaining the integrity of delayed-notice search warrants, we will seek the input of the Justice Department on the "is likely to" standard before the bill is considered on the House floor and we hope the majority will be willing to make changes that may be sought by the Administration.

Despite this small step towards compromise, the Majority took no further steps to limit the additional damage this legislation wreaks upon the statute as currently written. Section 106 still amends the provision that requires that notice of a delayed search warrant be given within a reasonable period. Under current law, the government must inform the target of the search within thirty days. This legislation only allows seven days.

Lastly, section 106 still amends the provision that allows the government to extend the period of delay in notifying the target of the search, if there is a need to do so. Under current law, the gov-

---

[10] *See Dalia v. United States,* 441 U.S. 238 (1979); *see also Katz v. United States,* 389 U.S. 347 (1967).

[11] April 4, 2005 U.S. Department of Justice letter to Senator Specter. p. 3 citing *United States v. Freitas,* 800 F.2d 1451 (9th Cir. 1986); *United States v. Villegas,* 899 F.2d 1324 (2d Cir. 1990); *United States v. Simons,* 206 F.3d 392 (4th Cir. 2000).

ernment may show cause to the court that the facts of the case necessitate further delay, for up to ninety days. This legislation mandates that the United States Attorney (and not a designee) for the district in which an extension order is sought make a written application to the court for further delays of not more than twenty-one days. Also, the court can only grant the application if it once again looks into the future and makes a finding that the extended delay is necessary because notice to the target of the search will result in (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; or (4) intimidation of potential witnesses.

The changes to this authority create substantial new burdens for law enforcement officials to overcome if they wish use delayed notice search warrants. The section also unduly limits the court's discretion in granting or extending delayed notice warrants. All of this is done without any evidence of past abuse of this limited authority. Section 106 is the very definition of change for the sake of change.

Criminal Pen Register and Trap and Trace Devices

The criminal code has provided Federal law enforcement agencies with the authority to use pen registers and trap and trace devices since 1986. The code also authorizes State and local law enforcement officers to make an application to a State court for use of these tools in State criminal investigations, where authorized.

The current standard for a pen register is that "the information likely to be obtained is relevant to an ongoing criminal investigation by that agency." As introduced, section 107 amended the standard to require a "statement of 'specific and articulable facts' by the applicant to justify the belief of the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."

The underlying bill unnecessarily elevates the standard for criminal pen registers and trap and trace devices. There is no evidence of any abuse of this *criminal* authority and therefore there was no reason to amend this provision at all, and certainly not in a reauthorization of the USA PATRIOT Act.

Use of a pen register or trap and trace device is not a search under the fourth amendment because the devices *do not allow the collection of any content.* As the Supreme Court noted in 1979, "Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers." [12]

For reasons beyond our understanding, the bill and the manager's amendment apply these proposed changes to all Federal, State, and local criminal investigations—well beyond the limited scope of FISA. The majority initially ignored the strong opposition of the National District Attorneys Association, the National Sheriffs' Association, the Fraternal Order of Police, and the Inter-

[12] *Smith v. Maryland,* 442 U.S. 735, 741 (1979) (citations omitted).

national Association of Chiefs of Police, all of whom agreed that the proposed changes to criminal pen register and trap and trace devices would unduly burden State and local law enforcement agencies that regularly use these tools in State criminal investigations.

In an effort to preserve this long-standing investigative tool, Mr. Rooney offered an amendment to strike section 107 from the bill. The amendment was rejected by many of our colleagues in the majority and was ultimately defeated. However, a scant time later, Mr. Schiff offered an amendment to, inter alia, strike the section. In a remarkable turnaround, this amendment received the support of the majority and was approved. While we certainly do not approve of this method of legislating, we do approve of this final result.

FISA Pen Register and Trap and Trace Devices

Section 108, as introduced, amends the FISA pen register/trap and trace (PR/TT) standard to require "a statement of the specific and articulable facts 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 . . ."

Current law already imposes significant burdens on the government in its efforts to obtain pen registers in national security and terrorism cases. The government must already obtain court approval and certify that the information sought is foreign intelligence information or is relevant to an investigation to protect against terrorism.

Pen registers and trap and trace devices are not wiretaps. These tools *cannot be used to collect the content of communications.* FISA's PR/TT authority also explicitly safeguards first amendment rights. It requires that any "investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

Mr. Rooney offered an amendment to strike the heightened standard of specific and articulable facts from this section. We are pleased that the majority realized the significant limitations such a standard would place on the use of FISA PR/TT authority and approved Mr. Rooney's amendment.

Section 108, as introduced, also requires a PR/TT application to include a statement of proposed minimization procedures and requires the court to find that such procedures meet the definition. Minimization procedures are intended to limit the retention, and regulate the dissemination, of non-publicly available information concerning unconsenting U.S. persons, consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information. These procedures have traditionally been applied to criminal and FISA wiretaps, but in recent years were also applied to FISA business records orders.

Unlike with other minimization procedures in national security law, these procedures are unnecessary and unworkable, as pen register information by definition does not contain content. Under Federal law, information collected "shall not include the contents of any communication."

The manager's amendment offered by Chairman Conyers attempts to curb the breadth of PR/TT minimization by limiting its application to "extraordinary circumstances." Although this revised language narrows the instances in which the FISC may require minimization, the bill still requires the government to submit minimization procedures in every PR/TT application. This is extremely burdensome and unnecessary without any justification in the scant factual record developed by the Committee for such an important piece of legislation.

The changes in the manager's amendment do not resolve the overarching questions of (1) whether the government can even apply minimization procedures to PR/TT data; (2) how burdensome such a requirement will be the use of this tool; (3) has there been abuse or misuse of PR/TT authority and would any such misuse actually be corrected or alleviated through minimization? Congress should not revise FISA PR/TT authority without the answers to these questions.

Public Reporting on FISA

Section 6002 of IRTPA directs the Attorney General to provide semi-annual reports to the House and Senate Intelligence and Judiciary Committees providing, in part, the "aggregate number of persons targeted for orders issued under FISA, including a breakdown of (1) electronic surveillance, (2) physical searches, (3) pen registers, (4) business record orders, (5) acquisitions inside the U.S. of persons located outside the U.S., and (6) other acquisitions targeting U.S. persons outside the U.S.

Section 109 of the bill requires the Attorney General to make this information publicly available. This is yet another attempt by the majority to "declassify" sensitive, national security information. There is no need to make such reports public. First, this change is unnecessary for Congress' oversight purposes. The committees of jurisdiction already receive bi-annual classified reports under this requirement. Second, this information is classified and the authority to declassify information rests with the President, not Congress. Congress cannot circumvent this reality simply by dictating public release of classified information in a statute. Third, the amendment requires the carte blanche release of all information in the bi-annual reports with no regard as to whether such information should be divulged or to what extent. Declassifying this information does not just make it available to the American people. It makes it available to our enemies as well.

It would be careless of Congress, under the guise of transparency, to require the public reporting of highly classified information. To this end, Mr. Coble offered an amendment to strike section 109. After receiving assurances from Chairman Conyers that we would work in a bipartisan fashion with the Justice Department to determine what, if any, information can be released publicly, Mr. Coble withdrew his amendment. We will work with the majority before the bill comes before the full House to resolve this substantively and constitutionally defective provision.

Sunset

Section 202 sunsets current national security letter authority on December 31, 2013, with the effect of returning the relevant national security letter statutes to their pre-9/11 standard ((1) relevant to an authorized investigation, and (2) that the FBI had specific and articulable facts giving reason to believe that information requested pertained to a foreign power or agent of a foreign power, such as a terrorist or a spy)). Through an audit covering the years 2003 to 2005, inaccuracies were found in records related to the issuance and reporting of NSLs and violations of procedures in place to govern the issuance, use, and oversight of NSLs. This naturally caused great concern in Congress and at the highest level of the FBI evoking efforts to correct and better oversee the use of this important law enforcement tool.

It would be understandable if the purpose of the sunset were to provide leverage to demand accountability and give Congress oversight. However, indications by the majority appear to reflect a desire to actually return to the old standard—requiring 'specific and articulable facts' that the information pertained to a foreign government, terrorist, or spy. This prior standard prevented investigators from acquiring records that were relevant to an ongoing international terrorism or espionage investigation. It makes no sense to roll back the 2001 reforms for NSLs. Criminal investigators have long been able to use grand jury subpoenas to obtain many of the same records so long as they are relevant to their investigation. Why should we have a more stringent standard for national security investigations?

Standard

Section 204 of the bill requires an official with authority to issue a national security letter to document and retain, *in a separate writing,* a statement of "specific and articulable facts" showing that there are reasonable grounds to believe that the information sought pertains to a foreign power or agent of a foreign power.

This standard effectively changes the focus of the "relevance" required under current law from "relevant to an authorized investigation" to "pertaining to" a "foreign power or agent of a foreign power." In addition, current law does not directly couple the relevance standard with "specific and articulable" facts as support for relevance—thus creating a more exacting standard for the government to meet which will inevitably limit the scope of information that the government can seek even if it is related to an authorized national security investigation. This requirement keeps the FBI from using NSLs to develop evidence at the early stages of an investigation, when they are the most useful, that can be used to establish links between terrorists, terrorist funding support, or those engaged in espionage, because it has not yet been established that they are related to a foreign power or an agent of a foreign power.

By requiring a separate writing documenting specific and articulable facts that information sought pertains to a foreign power or agent of a foreign power, it effectively rolls back the standard for NSLs to the pre-USA PATRIOT Act standard without explicitly doing so in the NSL certification to the NSL recipient.

Current law also does not require the government to create and maintain a record of such facts at the time the national security letter is issued.

National Security Letters are similar to administrative subpoenas, which almost universally require only a showing of relevance to the particular investigation; thus the change to the NSL standard in the original USA PATRIOT Act.

Mr. Chaffetz offered an amendment to strike section 204, but it was rejected by the majority. We find it ironic that the majority insists upon a heightened standard for foreign intelligence and terrorism investigations, yet just recently overwhelmingly approved a significantly lower standard for certain health care investigations. Section 1640 of H.R. 3962, the Affordable Health Care for America Act, allows the Department of Health and Human Services to issue administrative subpoenas to insurance companies during investigations of decisions to exclude benefits.

The standard for issuing an administrative subpoena under H.R. 3962 is extremely low. The information sought must simply "relate to" the matter under investigation—a standard well below the current relevance standard for NSLs and most administrative subpoenas. It is important for the American people to understand this distinction. The majority wants to make it easier for the government to investigate insurance companies than to investigate terrorists plotting to kill Americans.

Disclosure for Law Enforcement Purposes

Section 206 requires the Attorney General to authorize the use of any information acquired or derived from a national security letter in a criminal proceeding. For reasons beyond our comprehension, the majority appears to believe that the third-party records obtained through a NSL in a counter-terrorism or intelligence investigation should not be used in a terrorism or espionage trial. Why does the majority want to hinder the prosecution of terrorists and spies? Current law does not require such authorization for NSLs because the information obtained through NSLs, like the information obtained through a grand jury or administrative subpoena, is entirely admissible in a criminal trial.

The manager's amendment amends section 206 to allow the Attorney General to delegate this disclosure authority to other officials, but only one that has attained the rank of Section Chief of a division of the Department of Justice. The amendment also deletes language that would have required such authorization for the use of any information *derived from* a NSL.

These changes do little to alleviate the devastating effects of this provision. Perhaps the single most important lesson of 9/11 was the importance of allowing our law enforcement and national security investigators to share information in order to detect and stop terrorists before they strike.

This section creates administrative hurdles that make it much more difficult for intelligence agents to share information they obtained via a national security letter with their law enforcement brethren. By creating these extra steps for approving disclosure of certain information, the Committee will likely ensure that national security agents will avoid the hassle of the disclosure process.

When Congress passed the USA PATRIOT Act, we recognized that artificial legal walls between these criminal and national security agents, whether real or perceived, were an impediment to effective criminal and national security investigations.

For more than eight years, Members of Congress have reiterated that effective and timely information sharing is critical to effective investigations, even among investigators and prosecutors with seemingly divergent missions. Congress has demanded nothing less than complete and open information sharing between such investigations to protect the American people and prevent another event like the 9/11 attacks.

Despite this consistent mandate since 9/11, the majority now seems intent upon sending the opposite message and is demanding that law enforcement officials once again erect internal walls that compartmentalize information gathered from counterterrorism and counterintelligence investigations from use in criminal investigations or proceedings.

Judicial Review of National Security Letter Nondisclosure Order

Section 207 establishes additional procedures for a recipient to seek judicial review of a nondisclosure requirement imposed in connection with a national security letter. If the recipient wishes to have a court review a nondisclosure requirement, the recipient must notify the government. Not later than thirty days after the receipt of notification, the government must apply for a court order prohibiting the disclosure of information about the national security letter or the existence of the national security letter.

The nondisclosure requirement remains in effect during the pendency of any judicial review proceedings. The government's application for a nondisclosure order must include a certification from the Attorney General, Deputy Attorney General, or the Director of the FBI (or the head of another agency if not part of DOJ) containing a statement of specific and articulable facts indicating 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. If a court determines that there is reason to believe that disclosure will result in one of the enumerated harms, the court "may" issue a nondisclosure order for no longer than 180 days, *but a court could still refuse to do so with the current language.*

The government can seek renewals of nondisclosure orders for additional periods of not longer than 180 days each. If there comes a time when the facts supporting a nondisclosure order issued by the court cease to exist, this section requires the government to promptly notify a recipient who sought judicial review of a nondisclosure order that the nondisclosure is no longer in effect.

Most of Section 207 is aimed at codifying *Doe v. Mukasey*[13] which held that open-ended nondisclosure requirements for NSL recipients without meaningful judicial review are an unconstitutional prior restraint on the first amendment speech of the recipient. It further held that while high level government official certifi-

[13] 549 F.3d 861 (2nd Cir. 2008)

cations regarding the potential harms from disclosure could be provided deference by reviewing district courts, they could not be a "conclusive certification" precluding meaningful district court review of the potential harms if the recipient challenged. The FBI currently provides notice of right to judicial review and initiates timely judicial review upon request by the recipient of any NSL pursuant to *Doe v. Mukasey*.

This section, however, goes well beyond the mandate in *Doe* or the current procedures provided by the FBI pursuant to *Doe*. First, this section requires the government to provide to the court in its initiation of judicial review a "statement of specific and articulable facts indicating that, absent a prohibition of disclosure under this section, there 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."Neither current law nor this bill requires "specific and articulable facts" be provided to the recipient to justify the initial non-disclosure. The current standard is "certifies that [in the absence of nondisclosure] there may result [an enumerated harm]."

Moreover, this bill provides no deference to the government in the standard to be used by the court in reviewing a challenge to a nondisclosure order. Although *Doe* rejected the concept of a conclusive certification by the government, it most certainly advocated deference to the government. Specifically, the court interpreted the statute "to place on the Government the burden to show a "good" reason to believe that disclosure may result in an enumerated harm . . . and to place on a district court an obligation to make the 'may result' finding only after consideration, albeit deferential, of the Government's explanation concerning the risk of an enumerated harm."

This section also attempts to limit renewal of nondisclosure to 180 days. So, even if the government prevails in meeting its burden for the nondisclosure order, such an order will only extend for an additional 180 days and the court must make a separate finding that the government's reason for nondisclosure justifies the renewal of such order.

We have no objection to language that accurately codifies the court's remedy in *Doe*. However, this section goes well beyond *Doe* and for no apparent reason except change for the sake of change. We oppose these additional and unnecessary requirements on judicial review of NSL non-disclosure.

Minimization Procedures

Section 208, as introduced, requires the Attorney General to establish minimization procedures to limit the acquisition and retention of, and prohibit dissemination of, information obtained on non-consenting U.S. persons through NSLs—consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence. Section 208 also requires that the minimization procedures be transmitted to the House and Senate Judiciary Committees and the House and Senate Intelligence Committees within three months of bill passage.

This language made reference to minimizing NSLs in "light of the purpose and technique of the particular *surveillance*." NSLs

neither authorize nor acquire any surveillance, electronic, physical or otherwise.

In addition to creating significant and ongoing administrative review of every case in which an NSL is used (while simultaneously limiting the scope of NSLs) in order to identify any information received relating to a United States person *not believed to be an agent of a foreign power,* it requires deadlines for the destruction, minimization, or return of that information, even if that information is relevant to or necessary to understand foreign intelligence or a national security investigation.

The manager's amendment modifies the minimization language to delete the reference to NSLs as "surveillance" and removes the requirement that certain information be destroyed. However, it continues to impose unworkable, burdensome requirements on the acquisition, retention and dissemination of NSL-obtained information that will significantly curtail the use of NSLs in counter-terrorism and intelligence investigations.

Conclusion

America is fortunate to not have suffered a terrorist attack on our soil in over eight years. This good fortune was not achieved by chance but by hard work, and we must not let our safety become complacency. America is safe today not because terrorists and spies have given up their mission to destroy our freedoms and our way of life. America is safe today because the men and women of the intelligence community use the tools provided to them under the USA PATRIOT Act and other intelligence laws to protect us. It would be irresponsible of Congress to take away or weaken the authorities needed to their job.

Despite corrections to certain provisions in this bill, such as the standard for FISA business records and criminal and FISA pen registers, H.R. 3845 still suffers from numerous problems. The majority seeks to rewrite important foreign intelligence laws under the guise of civil liberty protections with no demonstrable evidence that such changes will, in fact, accomplish this goal. What we do know is that these changes for the sake of change risk diminishing or preventing the use of intelligence-collection measures that have protected America for eight years. We urge our colleagues to oppose this legislation and support instead legislation that simply reauthorizes the expiring provisions of current law, as proposed by Republican members of this Committee and by the Obama Administration.

LAMAR SMITH.
F. JAMES SENSENBRENNER, JR.
HOWARD COBLE.
ELTON GALLEGLY.
BOB GOODLATTE.
DANIEL E. LUNGREN.
DARRELL E. ISSA.
J. RANDY FORBES.
STEVE KING.
TRENT FRANKS.
LOUIE GOHMERT.
JIM JORDAN.
TED POE.

JASON CHAFFETZ.
TOM ROONEY.
GREGG HARPER.

○