

[Floor Situation](#) | [Summary](#) | [Background](#) | [Cost](#) | [Staff Contact](#)

[H.R. 2048, Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring \(USA FREEDOM\) Act of 2015](#)

FLOOR SITUATION

On Wednesday, May 13, 2015, the House will consider [H.R. 2048](#), *the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015*, under a [closed rule](#). H.R. 2048 was introduced on April 28, 2015, by Rep. James Sensenbrenner (R-WI) and was referred to the Committee on the Judiciary, and in addition to the Committees on Intelligence and Financial Services. The Judiciary Committee ordered the bill reported by a vote of [25 to 2](#) on April 30, 2015.

SUMMARY

H.R. 2048 includes numerous reforms to the nation's intelligence-gathering programs operated under the Foreign Intelligence Surveillance Act (FISA). The bill builds on legislation (H.R. 3361) passed in the 113th Congress to reform surveillance authorities and strengthen privacy and civil liberties protections.

The bill is designed to:

- End the bulk collection of data by prohibiting bulk collection of all records under Section 215 of the PATRIOT Act, the FISA pen register authority, and national security letter statutes.
- Prevent government overreach by prohibiting large-scale, indiscriminate collection of metadata, such as all records from an entire state, city, or zip code.
- Strengthen protections for civil liberties by creating a panel of experts to advise the FISA court on matters of privacy and civil liberties, communications technology, and other technical or legal matters.
- Increase transparency by requiring the declassification and disclosure of all significant opinions of the FISA court.
- Protect national security by closing loopholes that currently make it difficult to track foreign terrorists as they enter and leave the country, clarifying the application of FISA to foreign targets who facilitate the international proliferation of weapons of mass destruction, increasing

the maximum penalties for material support of a foreign terrorist organization, and extending the sunsets of the expiring PATRIOT Act provisions to December 2019.

Title I—FISA Business Records Reforms

Section 101—Additional requirements for detail records

Establishes a new, narrowly-tailored mechanism for the targeted collection of telephone metadata for possible connections between foreign powers or agents of foreign powers and others as part of an authorized investigation to protect against international terrorism. If the government can demonstrate a reasonable, articulable suspicion that a specific selection term is associated with a foreign power or an agent of a foreign power engaged in international terrorism, the Foreign Intelligence Surveillance Court (FISC) may issue an order for the ongoing, daily production of call detail records held by telephone companies for up to two hops.¹

The substantive limit will restrict the results of queries of telephony metadata to two “hops” away from the initial telephone number that is used as the starting point of the query. A “hop” is a colloquial term for a connection between two telephone numbers. So a two-hop limit will allow the NSA to retrieve all the contacts a queried number has made (1st hop) as well as all the contacts each of the 1st hop numbers has made.²

The term “call detail records” include session-identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity number, or an International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call.” The bill explicitly excludes from that term the contents of any communication; the name, address, or financial information of a subscriber or customer; and cell site location or GPS information.

The prospective collection of call detail records is limited to 180 days and may be renewed through the FISC.

Section 102—Emergency authority

Creates a new emergency authority for the use of Section 501. The Attorney General may authorize the emergency production of tangible things, provided that such an application is presented to the court within seven days. If the court denies an emergency application, the government may not use any of the information obtained under the emergency authority except in instances of a threat of death or serious bodily harm.

Section 103—Prohibition on bulk collection of tangible things

Provides that Section 501 may only be used where a specific selection term is provided as the basis for the production of tangible things. Makes clear that the government may not engage in indiscriminate bulk collection of any tangible thing under Section 501 of FISA.

Section 104—Judicial review

¹ As with the first “hop,” a second “hop” cannot be based on, nor return, cell site or GPS location information. It also does not include an individual listed in a telephone contact list, or on a personal device that uses the same wireless router as the seed, or that has similar calling patterns as the seed. Nor does it exist merely because a personal device has been in the proximity of another personal device. These types of information are not maintained by telecommunications carriers in the normal course of business and, regardless, are prohibited under the definition of “call detail records.”

² See CRS Legal Sidebar—“[President Obama Announces Changes to NSA Telephony Metadata Program](#),” January 23, 2014.

Provides that the Court may evaluate the adequacy of minimization procedures under Section 501. Under current law, the Court is only empowered to determine whether the government has minimization procedures in place. This section makes clear that the FISC may require additional, particularized minimization procedures beyond those required under Section 501.

Section 105—Liability protection

Provides liability protections to third parties who provide information, facilities, or technical assistance to the government in compliance with an order issued under Section 501.

Section 106—Compensation for assistance

Permits the government to compensate third parties for producing tangible things or providing information, facilities, or technical assistance in accordance with an order issued under Section 501.

Section 107—Definitions

Defines the terms “address,” “call detail record,” and “specific selection term.”

Section 108—Inspector General reports on business records orders

Requires the Inspector General of the Department of Justice to conduct a comprehensive review of the use of Section 501 with respect to calendar years 2012 to 2014. Also requires the Inspector General of the Intelligence Community to assess the value and use of intelligence obtained under Section 501 over the same period.

Section 109—Effective date

Provides that the new call detail records authority, the new Section 501 emergency authority, and the prohibition on bulk collection of tangible things under Section 501 take effect 180 days after enactment.

Section 110—Rule of Construction

Provides a rule of construction that nothing in this Act shall be construed to authorize the production of the contents of electronic communications by electronic communication service providers under Title V of FISA.

Title II—FISA Pen Register and Trap and Trace Device Reform

Section 201—Prohibition on bulk collection

Prohibits the use of the pen register and trap and trace device authority for bulk collection by requiring each application under this section to include a specific selection term as the basis for their use.

Section 202—Privacy procedures

Directs the Attorney General to adopt procedures to safeguard non-publicly available information concerning U.S. persons consistent with the need to protect national security. Clarifies that the FISC may require additional privacy or minimization procedures with regard to the installation or use of a pen register or trap and trace device.

Title III—FISA Acquisitions Targeting Persons Outside the United States Reforms

Section 301—Limits on use of unlawfully obtained information

Precludes the government's use of information acquired under Section 702 of FISA outside the scope of court-approved targeting and minimization procedures.

Title IV—Foreign Intelligence Surveillance Court Reforms

Section 401—Appointment of amicus curiae

Provides that both the FISC and the FISA Court of Review (FISCR) shall, if deemed appropriate, appoint an individual to serve as amicus curiae in a case involving a novel or significant interpretation of law. Permits the court to appoint amicus curiae in any case. The presiding judges of the courts will designate no fewer than five individuals who are eligible to serve as amicus curiae. These individuals shall possess expertise in privacy and civil liberties, intelligence collection, telecommunications, or any other area that may lend legal or technical expertise to the courts, and shall be eligible for access to classified information necessary to participate as amicus curiae.

Section 402—Declassification of decisions, orders, and opinions

Requires the Attorney General to conduct a declassification review of each decision, order, or opinion of the FISC or FISCR that includes a significant construction or interpretation of law. In the interest of national security, the Director of National Intelligence (DNI) may waive the declassification requirement, in which case the Attorney General shall provide a summary of the decision.

Title V—National Security Letter Reform

Section 501—Prohibition on bulk collection

Prohibits the use of various National Security Letter (NSL) authorities without the use of a specific selection term as the basis for the national security letter request. Specifies that for each NSL authority, the government must specifically identify the target or account.

Section 502—Limitations on disclosure of national security letters

Permits the government to impose a nondisclosure order on the recipient of an NSL if a senior FBI official certifies that danger to the national security, or danger to the life or safety of a person may result from public disclosure of the order. Allows the recipient of an NSL nondisclosure order to challenge order by notifying the government or by filing a petition for judicial review. Requires the government to periodically review standing NSL nondisclosure orders to determine if they are still necessary.

Section 503—Judicial review

Modifies each of the national security letter statutes to specify that judicial review of NSLs and nondisclosure orders is governed by 18 U.S.C., Section 3511, and that each NSL issued shall notify the recipient of the availability of judicial review of the NSL itself, as well as of the nondisclosure order.

Title VI—FISA Transparency and Reporting Requirements

Section 601—Additional reporting on orders requiring production of business records; business records compliance reports to Congress

In addition to existing annual reporting requirements, requires the government to provide to Congress: a summary of all compliance reports related to the use of Section 501; the number

of applications made for call detail records under the new call detail record authority, including the number granted, modified, or denied; the number of standard Section 501 applications and orders granted, modified, or denied; and the number of Section 501 applications based on a specific selection term that does not specifically identify an individual, account, or personal device, including whether they were granted, modified, or denied (and for those granted or modified) whether the FISC adopted additional, particularized minimization procedures.

Section 602—Annual reports by the Government

Requires the Administrative Office of the United States Court to report annually on the number of orders issued under sections 105, 304, 402, 501, 702, 703, and 704 of FISA, as well as on the number of appointments of individuals to serve as amicus curiae to the FISA court, and on the instances in which the FISC issued a finding that such appointment was not appropriate. The section also requires the government to report annually to the public key information about the scope of collection under the FISA pen register, business records, call detail records, and Section 702 authorities, as well as NSL statutes.

Section 603—Public reporting by persons subject to FISA orders

Permits any company that is subject to a FISA order or an NSL to publicly report information about the number of orders or NSLs it receives and how many of its customers are targeted by these national security processes.

Section 604—Reporting requirements for decisions, orders, and opinions of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review

Requires the Attorney General to provide to the relevant congressional committees, within 45 days, a copy of each decision, order, or opinion, including a modification or denial of an application that includes a significant construction or interpretation of any provision of law.

Section 605—Submission of reports under FISA

Includes the House Committee on the Judiciary in several existing reporting requirements.

Title VII—Enhanced National Security Provisions

Section 701—Emergencies involving non-U.S. persons

Provides for the lawful targeting of a non-United States person who was previously believed to be located outside the U.S. for a period not to exceed 72 hours when it is determined that the non-U.S. person is reasonably believed to be located inside the United States, in certain limited circumstances. Among various requirements, the head of an element of the Intelligence Community must reasonably determine that a lapse in targeting such non-U.S. person poses a threat of death or serious bodily harm.

Section 702—Preservation of treatment of non-U.S. persons travelling outside the United States as agents of foreign powers

Addresses an anomaly in FISA that may be interpreted to require the government to terminate electronic surveillance under a probable cause Title I court order because a non-U.S. person, who is known to be acting inside the U.S. as an agent of a foreign power, travels temporarily outside the United States. A clarification to the definition of “agent of a foreign power” for non-U.S. persons ensures continuity.

Section 703—Improvement to investigations of international proliferation of weapons of mass destruction

Amends the definition of “agent of a foreign power” in FISA Section 101, pertaining to the international proliferation of weapons of mass destruction, to include those who aid and abet, or conspire with, persons engaged in such proliferation or activities in furtherance of such proliferation.

Section 704—Increase in penalties for material support of foreign terrorist organizations

Increases the statutory maximum penalty from 15 to 20 years for material support of designated foreign terrorist organizations.

Section 705—Sunsets

Reauthorizes Section 215 (business records) and Section 206 (roving wiretap authority) of the PATRIOT Act, and Section 6001 (lone wolf definition) of the Intelligence Reform and Terrorism Prevention Act of 2004, until December 15, 2019.

Title VIII—Safety of Maritime Navigation and Nuclear Terrorism Conventions Implementation

Sec. 801-805

These sections implement changes required by previously agreed-to protocols regarding maritime terrorism and navigation.

Sec. 811 and 812

These sections implement certain provisions of the Nuclear Terrorism Convention and the Convention on the Physical Protection of Nuclear Material.

BACKGROUND

The Foreign Intelligence Surveillance Act (FISA), enacted in 1978, provides a statutory framework by which government agencies may, when gathering foreign intelligence information, obtain authorization to conduct wiretapping or physical searches, utilize pen registers and trap and trace devices, or access specified business records and other tangible things. Authorization for such activities is typically obtained by court order from the [Foreign Intelligence Surveillance Court](#) (FISC), a specialized court created by FISA to act as a neutral judicial decision maker in the context of activities authorized by the statute.³ Following the September 11, 2001 terrorist attacks, Congress enacted the USA PATRIOT Act, which amended FISA and other statutes to expand the scope of federal authority for intelligence gathering. The law has since been reauthorized and revised.

In June 2013, Edward Snowden, a former defense contractor and CIA employee, released to the media classified material on top-secret National Security Agency (NSA) data collection programs, including a metadata program operated under Section 215 of the USA PATRIOT Act and a program called PRISM operated under Section 702 of the FISA Amendments Act. On June 5, 2013, it was reported that on April 25, 2013, the Foreign Intelligence Surveillance Court (FISC) granted an order requested by the FBI pursuant to Section 215 of the USA PATRIOT Act. The order compels a telephone service provider, on an “ongoing, daily basis,” to provide the NSA with “all call detail records or telephony metadata” for communications made via its systems, both within the United States and between the U.S. and other countries. “Telephony metadata” is broadly defined, and

³ See CRS Report—“[Reauthorization of the FISA Amendments Act](#),” April 8, 2013 at 1.

includes the numbers of both parties on a call, unique identifiers, and the time and duration of all calls.⁴

On June 6, 2013, classified information regarding a second program, the PRISM program, was reported by the *Guardian* and *Washington Post*. PRISM was authorized by Section 702 of FISA, which was reauthorized by Congress in 2012 and expires in December of 2017. It allows the NSA to obtain data from electronic service providers regarding non-U.S. persons who reside outside the United States—including email, chat, photos, videos, stored data, and file transfers.⁵

A [White Paper](#) released by the Administration in August 2013 cited Section 215 of the Patriot Act as the legal authority for the metadata program.⁶ When it was enacted, Section 215 amended the procedures under FISA for obtaining records by expanding the range of records that could be sought to include “tangible things,” and by lowering the standard that had to be met before a court could issue an order.⁷ “The previous standard required a showing of specific and articulable facts giving reason to believe the information related to a foreign power or the agent of a foreign power. As amended [by the Patriot Act], the provision [requires] ‘a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to a [foreign intelligence, international terrorism, or espionage investigation].’”⁸

On January 17, 2014, President Obama announced reforms to the collection of signals intelligence by the Federal government⁹ and issued [Presidential Policy Directive](#) (PPD) 28. The Directive required that queries of telephone metadata collected by the NSA under Section 501 of FISA must first be approved by a FISC judge and that such queries would be limited to two “hops.”¹⁰

On May 7, 2015, a three-judge panel of the U.S. Court of Appeals for the Second Circuit [ruled](#) that the National Security Agency’s bulk collection of telephone metadata is not authorized under Section 215 of the PATRIOT Act. The Court declined to issue a preliminary injunction to halt the program while the lower court reconsiders the case, noting that “in light of the asserted national security interests at stake, we deem it prudent to pause to allow an opportunity for debate in Congress that may (or may not) profoundly alter the legal landscape.”¹¹ Section 215 is scheduled to expire on June 1, 2015.

The bulk collection of data under pen register and trap and trace authorities,¹² and the government’s use of National Security Letters (NSLs)¹³ to obtain information from telephone and internet

⁴ House Report 113-452, Part 1 at 13 and 14.

⁵ Id. at 14.

⁶ See CRS Legal Sidebar—“[NSA’s Telephone Metadata Program: Recent Developments](#),” April 15, 2013.

⁷ See CRS Report—“[Government Collection of Private Information: Background and Issues Related to the USA PATRIOT Act Reauthorization](#),” June 16, 2011 at 16.

⁸ Id.

⁹ <https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence>

¹⁰ Id.

¹¹ U.S. Court of Appeals for the Second Circuit, Docket No. 14-42cv, in [ACLU v. Clapper](#), May 7, 2015 at 95.

¹² “Pen registers capture the number dialed on a telephone line; trap and trace devices identify the originating number of an incoming call on a particular phone line.” Id. at FN 30.

¹³ “National Security Letters are regularly used in FBI counterterrorism investigations and are roughly comparable to administrative subpoenas. They have been described as ‘form letters signed by an FBI agent’ used to request and collect non-content consumer records and related information from ‘telephone companies, Internet service providers, consumer credit reporting agencies, banks, and other financial institutions.’” See Congressional Research Service Report—“[The Federal Bureau of Investigation and Terrorism Investigations](#),” February 19, 2014 at 6.

companies, has also garnered significant attention since disclosures about the NSA's surveillance program. In recent years, nondisclosure orders have been applied to 97% of NSLs, generally prohibiting the recipient from disclosing the information request.

In the 113th Congress, the House approved a similar bill ([H.R. 3361](#)) by a vote of [303 to 121](#) on May 22, 2014.

COST

The Congressional Budget Office (CBO) [estimates](#) that implementing H.R. 2048 would cost \$15 million over the 2016 to 2020 period, subject to the appropriation of the necessary amounts. CBO does not provide estimates for the cost of classified programs; therefore, this estimate addresses only the unclassified aspects of the bill.

ADDITIONAL INFORMATION

For additional information, please see the following materials prepared by the Committee on the Judiciary:

- [Fact Sheet](#)
- [Chart](#) of key differences between H.R. 2048 and H.R. 3361 from 113th Congress

STAFF CONTACT

For questions or further information please contact [Jerry White](#) with the House Republican Policy Committee by email or at 5-0190.