THE USA FREEDOM ACT OF 2013: SECTION-BY-SECTION ANALYSIS

Sec. 1. Short Title.

- The short title of the bill is the "Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring Act," or the USA FREEDOM Act.

Title I: FISA Business Records Reforms

Sec. 101. Privacy protections for section 215 business records orders.

- This section ends bulk collection under Section 215 of the USA PATRIOT Act by elevating the standard the government must meet to obtain a court order for tangible things under that provision. Current law requires the government to submit a statement of facts showing reasonable grounds to believe that the tangible things or records sought are relevant to an authorized investigation. The executive branch has argued and the FISA Court has accepted that this standard authorizes the bulk collection of Americans' phone records under Section 215.

- This section instead requires the government to show that the tangible things sought under this authority are relevant and material to an authorized investigation and that they pertain to (a) a foreign power or an agent of a foreign power, (b) the activities of a suspected agent of a foreign power who is the subject of such an authorized investigation, or (c) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation. This requires the government to show that the individual whose records it seeks has some connection to terrorism or espionage before it can obtain those records – and effectively ends bulk collection.

- This section also requires court review of minimization procedures for information obtained under Section 215.

- This section permits the court to impose a nondisclosure order for a specified period of time on the recipient of a Section 215 order if the court finds that certain harms are likely to result from public disclosure of the order and that the gag is narrowly tailored to address those harms. That nondisclosure order could be extended by the court an unlimited number of times if the government demonstrates that an extension is necessary.

- This section allows the recipient of a Section 215 order for tangible things to challenge the order itself and any nondisclosure order associated with it. Current law requires a recipient to wait a year before challenging a nondisclosure order in court. This section repeals that one-year mandated delay. It also repeals a provision stating that a conclusive presumption in favor of the government shall apply where a high level official certifies

that disclosure of the order for tangible things would endanger national security or interfere with diplomatic relations.

- This section adds a new authority similar to those found in other parts of the FISA to allow the government to obtain call detail records (but not including content or location information) without a court order if the Attorney General determines that an emergency requires their production before a court order can be obtained. An application must be filed with the court within seven days, and if the court denies the order the information obtained cannot be used or disclosed without consent or if the Attorney General finds that it indicates a threat of death or serious bodily harm.

Section 102: Inspector general reports on business records orders.

- This section requires the DOJ Office of Inspector General to conduct audits of the use of Section 215 of the USA PATRIOT Act. The audits will cover the years 2010 through 2013. The scope of such audits includes a comprehensive analysis of the effectiveness and use of the investigative authorities provided to the government, including any improper or illegal use of such authorities.

- This section also requires the Inspector General of the Intelligence Community to submit a report that reviews the implementation of this provision across the various agencies that make up the Intelligence Community.

Title II: FISA Pen Register and Trap and Trace Device Reforms

Section 201: Privacy protections for pen registers and trap and trace devices.

- This section ensures that the FISA pen register and trap and trace device (PR/TT) statute cannot be used to engage in bulk collection, as it has in the past. It replaces the current relevance standard with the same standard that Section 101 uses for Section 215 orders. This section requires the government to show that the information sought through the use of a PR/TT is relevant and material to an authorized investigation and pertains to (a) a foreign power or an agent of a foreign power, (b) the activities of a suspected agent of a foreign power who is the subject of such an authorized investigation, or (c) an individual in contact with, or known to, a suspected agent of a foreign power who is subject of such authorized investigation.

- This section also contains a new requirement for minimization procedures, and makes those procedures subject to court review.

Section 202: Inspector general reports on pen registers and trap and trace devices.

- This section requires the DOJ Office of Inspector General to conduct audits of the use of the FISA PR/TT authority. The audits will cover the years 2010 through 2013. The scope of such audits includes a comprehensive analysis of the effectiveness and use of the

investigative authorities provided to the government, including any improper or illegal use of such authorities.

- This section also requires the Inspector General of the Intelligence Community to submit a report that reviews the implementation of this provision across the various agencies that make up the Intelligence Community.

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

Section 301: Clarification on prohibition on searching of collections of communications to conduct warrantless searches for the communications of United States persons.

- Under Section 702 of FISA, which was enacted as part of the FISA Amendments Act (FAA), the government can wiretap foreigners outside the United States without a court order. This section closes NSA's "back door" access to Americans' communications by requiring a court order under FISA before the government can search for the communications of Americans in data collected without individualized warrants under Section 702. It contains an emergency exception like those found elsewhere in FISA.

Section 302: Protection against collection of wholly domestic communications.

- This section limits the circumstances in which the government can engage in so-called "about" collection. Under this type of collection, the government obtains communications "about" a target's account identifier (such as email address) – that is, communications that reference the account identifier in the contents of the communications but that are not to or from the target's account. This section permits this type of collection only to protect against international terrorism or the international proliferation of weapons of mass destruction.

Section 303: Prohibition on reverse targeting.

- This section places additional limits on the warrantless surveillance conducted under Section 702 to ensure that it is not used as a pretext when the government's real goal is to target the Americans with whom the foreign target is communicating. It requires a FISA Court order if the government is wiretapping a person overseas but "a significant purpose" of the surveillance is to collect the communications of the person in the United States with whom the person overseas is communicating.

Section 304: Limits on use of unlawfully obtained information.

- This section limits the government's use of information about U.S. persons that is obtained under Section 702 procedures that the FISA Court later determines to be unlawful, while still giving the FISA Court flexibility to allow such information to be used in appropriate cases. It is similar to the existing law that limits the use of

information collected pursuant to FISA's emergency authority if the FISA Court determines after the fact that the FISA standard was not met.

Section 305: Modification of FISA Amendments Act of 2008 sunset.

- This section amends the FISA Amendments Act, which was reauthorized in December 2012, to shorten the sunset from December 31, 2017, to June 1, 2015. The shortened FISA Amendments Act sunset would align with the sunset date for three PATRIOT Act provisions that expire on the same date (Section 215 orders; the "lone wolf" provision; "roving" wiretaps).

Section 306: Inspector general reviews of authorities.

- This section clarifies the scope of the authorization for reviews by the Inspectors General for those elements of the intelligence community that implement the FISA Amendments Act (Section 702 of FISA). It will ensure that such reviews cover any element that is subject to targeting or minimization procedures approved by the FISA court pursuant to Section 702.

- This section also requires a new independent review by the Inspector General for the Intelligence Community (IC IG). Under this section, the IC IG is required to review the procedures and guidelines developed by the intelligence community to implement this section, with respect to the protection of the privacy rights of U.S. persons. The IC IG review will include an evaluation of the limitations, procedures, and guidelines designed to protect U.S. person privacy rights, as well as an evaluation of the circumstances under which the contents of communications may be searched in order to review the communications of particular U.S. persons. The IC IG will be required to make publicly available a summary of the findings and conclusions of its review.

- This section also makes improvements to the annual review requirements for those elements of the intelligence community that implement Section 702 of FISA. It clarifies that annual reviews must be submitted by the head of any element in the intelligence community that is subject to targeting or minimization procedures approved by the FISA court pursuant to Section 702. This section also requires annual reviews of the number of targets that are later determined to be U.S. persons. Currently, the annual reviews only require a review of the number of targets later determined to be located within the United States.

Title IV: Foreign Intelligence Surveillance Court Reforms

Section 401: Office of the Special Advocate.

- This section creates the Office of the Special Advocate (OSA) as a part of the judicial branch. The Chief Justice appoints a Special Advocate for a 3-year renewable term from candidates nominated by the Privacy and Civil Liberties Oversight Board. The Special

Advocate and employees of the OSA are granted appropriate security clearances to carry out their duties.

- Under this section, the Special Advocate has access to all FISA applications, FISA Court decisions, and related material. The FISA Court may appoint the Special Advocate to participate in any proceeding, either *sua sponte* or after the Special Advocate has petitioned to participate. The Special Advocate may move the FISA Court to reconsider any decision, and reconsideration may be granted at the FISA Court's discretion. The Special Advocate may appeal decisions of the FISA Court to the FISA Court of Review, and may seek a writ of certiorari in the U.S. Supreme Court for review of decisions of the FISA Court of Review. The Special Advocate is responsible for advocating in support of legal interpretations that protect individual rights and civil liberties. The Special Advocate may also move the FISA Court to permit and facilitate amicus participation, which can also be done by the court *sua sponte*.

- This section requires the Attorney General to declassify or summarize FISA Court and FISA Court of Review decisions involving a significant construction or interpretation of law to the greatest extent consistent with legitimate national security considerations. The Attorney General must declassify documents sufficient to identify with particularity each legal question addressed by the decision and how such question was resolved; to describe in general terms the context in which the matter arises; to describe the construction or interpretation of any statute, constitutional provision, or other legal authority relied on by the decision; and to indicate whether the decision departed from any prior decision of the FISA Court or FISA Court of Review. The Special Advocate may petition the FISA courts to expand or modify the Attorney General's disclosures.

- This section requires the Special Advocate to report annually to Congress on the activities of the OSA and proposals for legislation that would improve the effectiveness of the OSA and the FISA system.

Section 402: Foreign Intelligence Surveillance Court disclosure of opinions.

- This section codifies FISA Court Rule of Procedure 62, which allows a FISA Court judge who authors an opinion *sua sponte* or by motion of a party to request that such opinion be made publicly available. Upon such request, the presiding judge of the FISA Court may consult with the other judges of the Court and direct that such opinion be made publicly available. Prior to making such opinion publicly available, the presiding judge may direct the executive branch to review it and redact it as necessary to protect classified information.

Section 403: Preservation of rights.

- This section provides that nothing in this act affects the authority of the FISA Courts to declassify decisions or release information, or the public's right to secure information under the Freedom of Information Act or other provisions of law.

Title V: National Security Letter Reforms

Section 501: National security letter authority.

- This section elevates the standard for national security letters (NSLs) to ensure the government does not use NSLs to conduct bulk collection of records. It requires that the records requested are relevant and material to an authorized investigation and that they pertain to (a) a foreign power or an agent of a foreign power, (b) the activities of a suspected agent of a foreign power who is the subject of such an authorized investigation, or (c) an individual in contact with, or known to, a suspected agent of a foreign power who is subject of such authorized investigation.

- This is the same standard imposed elsewhere in the bill for Section 215 orders and FISA pen register and trap and trace device orders – to ensure that any bulk collection program is not continued under the NSL authority.

- This section also specifies the types of financial and consumer report records that can be obtained using NSLs, which do not require court approval. For financial records, it permits NSLs to be used to obtain the name and address of a customer, the length and type of service, and any account number or other identifier. It does not allow NSLs to be used to obtain the details of financial transactions. For consumer report records, the government can use NSLs to obtain names, current and former addresses, current and former places of employment, and name and address of any financial institution where the consumer has had an account. The government cannot obtain full consumer reports – which include extensive detail about consumers' financial history – with an NSL.

Section 502: Limitations on disclosure of national security letters.

- This section permits the government to impose a nondisclosure order for a specified period of time on the recipient of an NSL if a senior FBI official certifies that certain harms are likely to result from public disclosure of the order.

- This section corrects the constitutional defects in the issuance of NSL nondisclosure orders found by the Second Circuit Court of Appeals in *Doe v. Mukasey*, 549 F.3d 861 (2nd Cir. 2008), and adopts the concepts suggested by that court for a constitutionally sound process. It allows the recipient of an NSL nondisclosure order to challenge the nondisclosure order at any time by notifying the government of a desire not to comply, or by filing a petition for judicial review. If the recipient notifies the government, the government then has 30 days to seek a court order in federal district court to compel compliance with the nondisclosure order. This option is intended to ease the burden on the recipient in challenging the nondisclosure order. If the court determines there are reasonable grounds to believe that certain harms will result if the gag order is not imposed, the court shall issue the nondisclosure order. Requests for nondisclosure orders should be filed in the appropriate judicial district.

Section 503: Judicial review.

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

Section 504: Inspector general reports on national security letters.

- This section requires the DOJ Office of Inspector General to conduct audits of the use of national security letters. The audits will cover the years 2010 through 2013. The scope of such audits includes a comprehensive analysis of the effectiveness and use of the investigative authorities provided to the government, including any improper or illegal use of such authorities.

Section 505: National security letter sunset.

- This section adds new June 1, 2015, sunset provisions for statutes authorizing the use of national security letters. The new NSL sunsets would align with the sunset date for three PATRIOT Act provisions that expire on the same date (Section 215 orders; the "lone wolf" provision; "roving" wiretaps).

Section 506: Technical and conforming amendments.

- This section makes technical amendments relating to other changes made by this title.

Title VI: FISA and National Security Letter Transparency Reforms

Section 601: Third-party reporting on FISA orders and national security letters.

- Private companies are currently barred from disclosing basic information about the requests for information and assistance they receive from the government. Under this section, Internet and telecommunications companies are allowed to report publicly an estimate of: (1) the number of FISA orders and NSLs received; (2) the number of such orders and NSLs complied with; and (3) the number of users or accounts on whom information was demanded under the orders and letters. These estimates are rounded to the nearest 100.

Section 602: Government reporting on FISA orders.

- This section also requires the government to provide new public reporting on FISA implementation. Specifically, the government is required to make public reports estimating the total number of individuals and U.S. persons who were subject to various types of FISA orders, as well as the total number of U.S. persons whose information was

subsequently reviewed by a federal agent. These estimates are rounded to the nearest 100.

Section 603: Government reporting on national security letters.

- This section requires periodic unclassified reporting of aggregate NSL numbers based upon the total number of all NSLs issued each year. This section requires aggregate reporting as to various categories of NSL requests, including those that gather information about persons who are the subject of an authorized national security investigation, and about individuals who have been in contact with or otherwise directly linked to the subject of an authorized national security investigation.

Title VII: Privacy and Civil Liberties Oversight Board Subpoena Authority

Section 701: Privacy and Civil Liberties Oversight Board subpoena authority.

- This section permits the Privacy and Civil Liberties Oversight Board to issue subpoenas to non-governmental entities directly, without first submitting a written request to the Attorney General.

Title VIII: Severability

Section 801: Severability.

This section includes a severability clause.