

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
OAKLAND DIVISION

ELECTRONIC FRONTIER;)
FOUNDATION,)
)
Plaintiff,)
)
v.)
)
UNITED STATES DEPARTMENT OF JUSTICE,)
)
Defendant.)

Case No. 4:11-cv-05221-YGR

DECLARATION OF JENNIFER L. HUDSON
DIRECTOR, INFORMATION MANAGEMENT DIVISION,
OFFICE OF THE CHIEF INFORMATION OFFICER,
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Pursuant to 28 U.S.C. § 1746, I, Jennifer L. Hudson, declare the following to be true and correct:

1. I am the Director of the Information Management Division (“IMD”) for the Office of the Director of National Intelligence (“ODNI”). I have held this position since May, 2013. I joined ODNI in 2007 as the Chief, Information Review and Release Branch, and was directly involved in the creation of ODNI’s IMD. After a one-year assignment working in the ODNI’s Office of Legislative Affairs, I returned to IMD and assumed my current position as the Director of that office. Prior to my arrival in ODNI, I held information management positions in the Joint Personnel Recovery Agency, the Defense Prisoner of War/Missing Persons Office, and later in the Public Access Branch at the Defense Intelligence Agency.

2. IMD is responsible for facilitating the implementation of information

management-related Executive orders, laws, regulations, and ODNI policy. This function entails controlling information throughout its life cycle and includes the areas of records management, classification management and declassification, pre-publication reviews, and responding to requests under the Freedom of Information Act (“FOIA”) and the Privacy Act (“PA”).

3. Under a written delegation of authority by the Director of National Intelligence (“DNI”) pursuant to section 1.3(c) of Executive Order 13526, I hold original classification authority (“OCA”) at the TOP SECRET level. I am authorized, therefore, to conduct classification reviews and to make original classification and declassification decisions for intelligence information up to and including the TOP SECRET level. In my current position, I am the final decision-making authority regarding FOIA and PA processing for the ODNI/IMD.

4. Through the exercise of my official duties, I have become familiar with this civil action and the underlying FOIA request. I make the following statements based upon my personal knowledge and information made available to me in my official capacity.

5. I submit this declaration in support of the U.S. Department of Justice’s (“DoJ”) Motion for Summary Judgment in this proceeding. The purpose of this declaration is to explain and justify, to the extent possible on the public record, the actions taken by the Intelligence Community (“IC”) in responding to plaintiff’s request for information under the FOIA, 5 U.S.C. § 552, as well as describe the overall declassification review initiative that the IC is currently involved in concerning certain sensitive U.S. Government surveillance programs. Certain information regarding specific withholdings can only be explained in a classified declaration, and, as such, I have also executed a separate *ex parte, in camera* classified declaration dated March 28, 2014.

I. **ODNI BACKGROUND**

6. Congress created the position of the DNI in the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, §§ 1101(a) and 1097, 118 Stat. 3638, 3643-63, 3698-99 (2004) (amending Sections 102 through 104 of Title I of the National Security Act of 1947). Subject to the authority, direction, and control of the President, the DNI serves as the head of the IC, and as the principal adviser to the President and the National Security Council for intelligence matters related to the national security. 50 U.S.C. §§ 3023(b)(1), (2).

7. The responsibilities and authorities of the DNI are set forth in the National Security Act of 1947, as amended. These responsibilities include ensuring that national intelligence is provided to the President, heads of the departments and agencies of the Executive Branch, the Chairman of the Joint Chiefs of Staff and senior military commanders, and the Senate and House of Representatives and committees thereof. 50 U.S.C. § 3024(a)(1). The DNI is charged with establishing the objectives of; determining the requirements and priorities for; and managing and directing the tasking, collection, analysis, production, and dissemination of national intelligence by elements of the IC. 50 U.S.C. §§ 3024(f)(1)(A)(i) and (ii).

8. In addition, the National Security Act of 1947, as amended, provides that the DNI “shall protect intelligence sources and methods from unauthorized disclosure.” 50 U.S.C. § 3024(i)(1). Consistent with this responsibility, the DNI establishes and implements guidelines for the IC for the classification of information under applicable law, Executive orders, or other Presidential directives, and for access to and dissemination of intelligence. 50 U.S.C. § 3024(i)(2)(A), (B).

9. The function of the ODNI is to assist the DNI in carrying out his duties and responsibilities under the National Security Act and other applicable provisions of law, and to

carry out such other duties as may be prescribed by the President or by law.

II. PLAINTIFF'S FOIA REQUEST

10. By letter sent to the National Security Division ("NSD") of DoJ dated June 2, 2011, plaintiff, the Electronic Frontier Foundation ("EFF"), requested "agency records (including, but not limited to, electronic records) created from January 1, 2004 to the present discussing, concerning, or reflecting the DoJ or any of its components' interpretation or use of Section 215 orders."

11. By letter dated August 11, 2011, NSD informed EFF that it had searched its files and located responsive records, releasing three documents in full, but denying in full additional records based on FOIA Exemption 1.

12. By letter dated October 3, 2011, EFF appealed NSD's response. EFF then filed this lawsuit on October 26, 2011, before NSD could respond to EFF's appeal.

13. On February 10, 2012, the parties filed a stipulation that reflected plaintiff's agreement to narrow the scope of its request to include only:

- a. Legal opinions or memoranda concerning or interpreting Section 215 of the USA PATRIOT Act ("Section 215");¹
- b. Guidelines for government personnel regarding the use of Section 215;
- c. Reports provided to Congress by the Federal Bureau of Investigation ("FBI") or DoJ concerning or memorializing the Executive Branch's interpretation or use of Section 215;
- d. Reports, opinions, or memoranda of the Foreign Intelligence Surveillance Court ("FISC") concerning or interpreting Section 215; and

¹ The "business records" provision of the Foreign Intelligence Surveillance Act, enacted by Section 215, codified at 50 U.S.C. section 1861.

- e. Legal opinions or memoranda concerning or interpreting rulings, opinions, or memoranda of the FISC interpreting Section 215.

Plaintiff also agreed to exclude drafts of documents for which a final version was identified, electronic mail messages concerning drafts of documents, and the operational files of NSD's Office of Intelligence and its predecessor, Office of Intelligence Policy and Review.

14. In Part III of this declaration I will explain the overall declassification initiative that the IC is currently undertaking with respect to certain U.S. Government surveillance programs, and the re-processing of documents responsive to plaintiff's FOIA request and subject to continued litigation. In Part IV, I describe the continued withholdings by the IC and the basis for the FOIA exemptions asserted to support these withholdings. In Part V, I describe the segregability assessment made by the IC.

III. IC DECLASSIFICATION INITIATIVE AND RE-PROCESSING OF DOCUMENTS RESPONSIVE TO PLAINTIFF'S FOIA REQUEST

15. As the Court is aware, on or about June 6, 2013, *The Guardian* and *The Washington Post* published articles and documents received from former National Security Agency ("NSA") contractor Edward Snowden. This unprecedented unauthorized disclosure of TOP SECRET documents touched on some of the U.S. Government's most sensitive national security programs, including highly classified and on-going signals intelligence collection programs.

16. NSA's foreign intelligence mission includes the responsibility to collect, process, analyze, produce, and disseminate signals intelligence ("SIGINT") information, of which communications intelligence ("CI") is a significant subset, for (a) national foreign intelligence purposes, (b) counterintelligence purposes, and (c) the support of military operations. See E.O. 12333, section 1.7(c), as amended. In performing its SIGINT mission, NSA exploits foreign

electromagnetic signals to obtain intelligence information necessary to the national defense, national security, or the conduct of foreign affairs. Public disclosure of either the capability to collect specific communications or the substance of the information itself can easily alert targets to the vulnerability of their communications. Disclosure of even a single communication holds the potential of revealing the intelligence collection techniques that are applied against targets around the world. Once alerted, SIGINT targets can easily frustrate SIGINT collection by using different or new encryption techniques, disseminating disinformation, or by utilizing a different communications link. Such evasion techniques may inhibit access to the target's communications and, therefore, deny the United States access to information crucial to the defense of the United States both at home and abroad.

17. One of the greatest challenges the United States faces in combating international terrorism and preventing potentially catastrophic terrorist attacks on our country is identifying terrorist operatives and networks, particularly those operating within the United States. Detecting and preventing threats by exploiting terrorist communications has been, and continues to be, one of the tools in this effort. It is imperative that we have the capability to rapidly detect any terrorist threat inside the United States.

18. One method that the IC has developed to accomplish this task is analysis of metadata associated with telephone calls within, to, or from the United States under the Section 215 program. The term "telephony metadata" or "metadata" as used here refers to data collected under the 215 program that are about telephone calls—such as the initiating and receiving telephone numbers, and the time and duration of the calls—but does not include the content of those calls or any subscriber identifying information. By analyzing telephony metadata based on telephone numbers associated with terrorist activity, trained expert intelligence analysts can work

to determine whether known or suspected terrorists have been in contact with individuals in the United States.

19. The recent unauthorized disclosures include previously classified information regarding the Section 215 program. Under the Section 215 program, the FBI obtains orders from the FISC directing certain telecommunications service providers to produce all business records created by them (known as call detail records) that contain information about communications between telephone numbers, relating to telephone calls made between the United States and a foreign country and calls made entirely within the United States. The telephony metadata collection program was specifically developed to assist the U.S. Government in detecting such communications between known or suspected terrorists who are operating outside of the United States and who are communicating with others inside the United States, as well as communications between known or suspected terrorist operatives who are located within the United States.

20. As the FISC has observed, the production of all call detail records of all persons in the United States has never occurred under this program. By their terms, these FISC orders must be renewed approximately every 90 days. At least 15 different FISC judges have entered more than 35 orders authorizing NSA's bulk collection of telephony metadata under Section 215, including most recently on March 28, 2014.

21. The unauthorized disclosures regarding this program have caused exceptionally grave harm to our national security and threaten long-lasting and potentially irreversible harm to our ability to identify and respond to threats. In order to correct misinformation flowing from the unauthorized disclosures, and to reassure the American public as to the numerous safeguards that protect privacy and civil liberties, starting on June 6, 2013, the DNI declassified certain

information regarding the program authorized under Section 215, as well as other programs.

22. Cross-motions for summary judgment by the parties in this FOIA litigation were pending before the Court at the time of the unauthorized disclosures discussed above and the DNI's subsequent exercise of his discretion under E.O. 13526 to declassify certain information regarding the Section 215 program. Because of the likelihood that the DNI's declassification decision impacted the classification of documents responsive to plaintiff's FOIA request at issue in this case, the U.S. Government requested and the Court granted a stay of proceedings to permit the U.S. Government to reprocess the documents remaining at issue in this litigation.

23. In addition, to reassure the American people that the Section 215 program is lawfully authorized and operated, and to inform the discussion surrounding it, on June 20, 2013, the President directed the DNI to continue to review whether further information could be declassified, and to reassess the extent to which there may be information that can be released regarding the legal rationale, protections, and nature of the oversight of this surveillance program consistent with the interests of national security. *See* Section 3.1(c) and (d) of E.O. 13526. To that end, the DNI was directed to review, among other things, the FISC opinions and filings relevant to the program to determine what information could be declassified.

24. The U.S. Government has since engaged in a large-scale, multi-agency review process led by ODNI to determine what further information concerning programs under Section 215 and other surveillance programs could be declassified and released consistent with the national security for the purpose of restoring public confidence and better explaining the legal rationale and protections surrounding the programs. The latter consideration is a policy decision that must be weighed and decided at the highest levels of the U.S. Government. The overarching policy goal of this effort is to inform the public as much as possible, consistent with protecting

the national security, for the purpose of fostering an informed public debate and restoring public confidence that surveillance intelligence programs are lawful, properly authorized, and conducted in a manner consistent with the privacy and civil liberties of Americans.

Reprocessing of documents responsive to plaintiff's FOIA request was generally conducted as part of this broader review.

25. This review was extraordinarily complex and thorough. Relevant components of the national security community had to consider each piece of information identified for possible declassification and anticipate the ramifications such declassification might have on their operations, including the ability to gather intelligence in the future. An important component of the analysis was consideration of the information already in the public domain, and how official disclosures might allow our adversaries to fit new pieces of information together with those already in the public domain to create an even more revealing picture of our nation's intelligence capabilities, including its signals intelligence capabilities.

26. Consistent with this initiative, on September 10, 2013, September 17, 2013, October 11, 2013, October 28, 2013, November 18, 2013, January 17, 2014, and most recently on February 12, 2014, the DNI authorized, after the inter-agency review described above, the declassification and public release of a number of documents pertaining to telephony metadata collection under Section 215. These documents included documents responsive to plaintiff's FOIA request that were previously withheld in full as, *inter alia*, classified, as well as additional documents not responsive to plaintiff's request or part of this FOIA litigation. The DNI chose to exercise his discretion under E.O. 13526 to declassify certain information because he found extraordinary circumstances existed where the public interest in disclosure outweighed the harm to national security that would result. So far, approximately 2,400 pages of material related to

intelligence surveillance activities under the Section 215 program and other programs have been declassified and released to the public. They have all been made available on an ODNI website, IContheRecord.tumblr.com, which is designed to provide immediate, on-going, and direct access to factual information related to the lawful foreign surveillance activities carried out by the IC. It provides a single online location to access new information as it is made available from across the IC.

27. While the existence of the authority under Section 215 is set forth in public statutory provisions, and as stated above certain information about the program has been declassified, the operational details as to specific applications of the sources and methods used by the U.S. Government to carry out that authority remain highly classified. Likewise, information collected under this program is among the most important and valuable foreign intelligence information the U.S. Government collects, and is used to protect the country from a wide variety of terrorist threats.

IV. EXPLANATION OF WITHHELD MATERIAL

28. The purpose of this declaration is to advise the Court that the IC withheld certain information, as set forth below, because it is properly exempt from disclosure under the FOIA based on Exemptions 1, 3, 7(A) and 7(E), 5 U.S.C. §§552(b)(1), (3), (7)(A) and (7)(E), respectively. This is so because the information remains currently and properly classified in accordance with E.O. 13526 and protected from release by statutes, specifically Section 6 of the National Security Agency Act of 1959 (Pub. L. No. 86-36) (codified at 50 U.S.C. §3605) (“NSA Act”); and Section 102A(i)(1) of the National Security Act of 1947, as amended (codified at 50 U.S.C. § 3024(i)(1)), or is exempted from disclosure pursuant to Exemption 7(A) or 7(E) because it was compiled for law enforcement purposes and could reasonably be expected to

interfere with enforcement proceedings, or would disclose techniques and procedures for law enforcement investigations or prosecutions.

29. The records at issue for the renewed cross-motions for summary judgment are a representative sample of withheld documents consisting of all responsive Orders and Opinions of the FISC as agreed upon by the parties and set forth in the Joint Status Report and Proposed Schedule for Further Proceedings dated February 3, 2014 (hereinafter "Joint Status Report"). I am able to address the following FISC Orders and Opinions released in part in detail in this unclassified declaration: BR (business records) 06-05 Order dated May 24, 2006; BR 06-05 Order granting the U.S. Motion to Unseal Exhibit C-Memorandum of Law dated July 22, 2009; BR 08-13 Primary Order dated March 2, 2009; BR 08-13 Supplemental Opinion dated December 12, 2008; BR 08-13 Order Regarding Preliminary Notice of Compliance Incident dated January 28, 2009; PR/TT (pen register/trap and trace) [redacted] and BR 09-06 Order dated June 22, 2009 and PR/TT [redacted] Supplemental Order dated [redacted]; BR 09-13 Primary Order dated September 3, 2009; BR 09-13 Order Regarding Further Compliance Incidents dated September 25, 2009; BR 09-15 Supplemental Opinion and Order dated November 5, 2009, and BR 10-82 Supplemental Order dated November 23, 2010². I will also address in detail the following FISC Order denied in full: FISC BR 08-07 Supplemental Opinion, dated August 20, 2008. Finally, I will briefly address additional FISC Opinions or Orders that have been withheld in their entirety. For the Court's convenience, attached to this declaration as Exhibit A is an unclassified index of the documents still at issue in this case identifying, to the extent possible on the public record,

² I have been informed that plaintiff has agreed not to challenge the U.S. Government's withholdings in the above-referenced FISC Orders and Opinions from the following categories of information: targets of FBI investigations; identities of U.S. Government declarants; operational details about intelligence sources and the FISC's treatment of call detail records from such sources; operational details disclosing how the NSA obtains metadata from a specified service provider or providers; the code name of an FBI investigation; and the identities of FISC or other U.S. Government employees withheld pursuant to Exemptions 6 and 7(C). See Joint Status Report.

each document, its length, its date, and the applicable FOIA exemptions. For the Court's convenience, an unclassified *Vaughn* index of the withheld documents, providing as much detail as possible on the public record, is attached.

A. FOIA EXEMPTION 1

30. Exemption 1 of the FOIA protects from release matters that are specifically authorized under criteria established by an Executive order to be kept classified in the interest of the national defense or foreign policy, and are in fact properly classified pursuant to such Executive order. 5 U.S.C. § 552(b)(1). The current Executive order which establishes such criteria is E.O. 13526.

31. Section 1.1 of E.O. 13526 provides that information may be originally classified if: 1) an OCA is classifying the information; 2) the information is owned by, produced by or for, or is under the control of the U.S. Government; 3) the information falls within one or more of the categories of information listed in section 1.4 of the E.O.; and 4) the OCA determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, and the OCA is able to identify or describe the damage.

32. Section 1.2(a) of E.O. 13526 provides that information shall be classified at one of three levels. Information shall be classified at the TOP SECRET level if its unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the national security. Information shall be classified at the SECRET level if its unauthorized disclosure reasonably could be expected to cause serious damage to the national security. Information shall be classified at the CONFIDENTIAL level if its unauthorized disclosure reasonably could be expected to cause damage to the national security.

33. In addition, information shall not be considered for classification unless it falls

within one of the categories described in Section 1.4 of E.O. 13526. The relevant categories for purposes of this case are section 1.4(c), which allows information to be classified if it pertains to “intelligence activities (including covert action), intelligence sources or methods, or cryptology;” section 1.4(d), which include foreign relations or foreign activities of the United States, including confidential sources; and section 1.4(g), which include vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security.

B. FOIA EXEMPTION 3

34. Exemption 3 provides that FOIA does not require the production of records that are:

“specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A)(i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld; and (B) if enacted after the date of enactment of the OPEN FOIA Act of 2009, specifically cites to this paragraph.” 5 U.S.C. § 552(b)(3).³

35. The challenged information at issue here in this litigation falls squarely within the scope of two statutes. The first applicable statute is Section 102A(i)(1) of the National Security Act of 1947, as amended, 50 U.S.C. § 3024(i)(1), which provides that “the Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.” Like the protection afforded to core NSA activities by section 6 of the NSA Act, the protection afforded to intelligence sources and methods is absolute. Whether the sources and methods at issue are classified is irrelevant for purposes of the protection afforded by 50 U.S.C. § 3024(i)(1).

³ The OPEN FOIA Act of 2009 was enacted on October 28, 2009, Pub. L. 111-83, 123 Stat. 2142, 2184; 5 U.S.C. § 552(b)(3)(B), after the applicable National Security Act provision was enacted, and therefore is not applicable to the analysis in this case.

36. The second statute is a statutory privilege unique to NSA. As set forth in section 6 of the NSA Act, Public Law 86-36 (50 U.S.C. § 402 note), “[n]othing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, [or] of any information with respect to the activities thereof. . . .” (emphasis added). Congress, in enacting the language in this statute, decided that disclosure of any information relating to NSA activities is potentially harmful. Federal courts have held that the protection provided by this statutory privilege is, by its very terms, absolute. Section 6 states unequivocally that, notwithstanding any other law, including the FOIA, NSA cannot be compelled to disclose any information with respect to its activities. To invoke this privilege, the U.S. Government must demonstrate only that the information it seeks to protect falls within the scope of Section 6. Further, while in this case the harm would be exceptionally grave or serious, the U.S. Government is not required to demonstrate specific harm to national security when invoking this statutory privilege, but only to show that the information relates to its activities. NSA’s functions and activities are therefore protected from disclosure regardless of whether or not the information is classified.

37. As described above, these statutes protect the fragile nature of the U.S.’ intelligence sources, methods, and activities, to include but not limited to, the existence and depth of signals intelligence-related successes, weaknesses and exploitation techniques. These statutes recognize the vulnerability of intelligence sources and methods, including signals intelligence to countermeasures and the significance of the loss of valuable intelligence information to national policymakers and the IC. Given that Congress specifically prohibited the disclosure of the sources and methods used by the IC, as well as any information related to NSA’s functions and activities, I have determined that intelligence sources and methods,

including NSA's SIGINT activities and functions, would be revealed if any of the withheld information in the FISC's orders and opinions were released in part to the plaintiff.

38. All of the withheld information continues to require protection, notwithstanding the significant amount of information that has been declassified, as this withheld information, if disclosed, would provide our adversaries with the necessary information to develop countermeasures in an attempt to thwart the IC's collection sources and methods.

C. DOCUMENTS RELEASED IN PART

39. As indicated above, I am able to address 11 of the FISC Orders and Opinions released in part in this case in detail in this unclassified declaration because the facts justifying the withholdings in these documents are not themselves indicative of still classified intelligence sources, methods, and activities. The results of the IC declassification initiative discussed above permits this degree of detail regarding the justifications for the withholdings to now be provided here in this unclassified declaration. As discussed further below, some of the withholdings are made pursuant to FOIA Exemptions 1, 3, 7(A) and 7(E), and many fall into the categories of information that the plaintiff does not challenge, such as targets of investigations and the identities of personnel.

BR 06-05 Order dated May 24, 2006

40. All IC withholdings in this Order fall within the categories of information that plaintiff does not challenge per the Joint Status Report. Specifically, the information withheld by the IC in processing this Order under the FOIA for release to the plaintiff is the targets of the FBI investigations. The other redacted material was already embedded in the document as found by NSD when conducting its research for responsive records. This document is the copy that was provided to the Congressional intelligence committees pursuant to 50 U.S.C. §1871. Under this statute, the Attorney General ("AG"), in consultation with ODNI, may authorize redactions in

documents provided to Congress, which are limited to protect sensitive sources and methods or the identities of targets. In this document, the previously redacted information is the identity of the telecommunications provider, an intelligence source. Had this information not been previously redacted, the IC would have withheld this same information from release to the plaintiff because it is exempt from release based on FOIA Exemptions 1 and 3, as set forth in greater detail below in paragraphs 58-65.

BR 06-05 Order (to unseal Exhibit C-Memorandum of Law) dated July 22, 2009

41. All IC withholdings in this Order fall within the categories of information that plaintiff does not challenge per the Joint Status Report. Specifically, the information withheld by the IC in processing this Order under the FOIA for release to the plaintiff is the targets of the FBI investigations and the identity of a FISC employee whose name was withheld pursuant to FOIA Exemption 6.⁴

BR 08-13 Order dated March 2, 2009

42. This responsive Order is the version provided to the Congressional intelligence committees pursuant to 50 U.S.C. §1871, and it contains previously redacted information that the AG, in consultation with the DNI, authorized to be withheld in order to protect intelligence sources and methods, and identities of targets. This information consists of the telecommunications service providers who were ordered to produce all business records created by them that contain information about communications between telephone numbers, generally relating to telephone calls made between the United States and a foreign country and calls made

⁴ Exemption 6 provides that FOIA does not require the production of records that are "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). I understand the plaintiff is not challenging redactions made to protect the names of U.S. Government employees, including employees of the FISC, pursuant to Exemption 6.

entirely within the United States (see paragraphs 58-65 below) and the targets of the FBI investigations, which plaintiff is not challenging. This Order was processed in the Summer of 2013, and there is one piece of previously-redacted information in this Order that can now be released based on the President's transparency initiative. This information is the phrase "those companies" which is found on page 1, line 5. This piece of information meets the criteria for classification, however, after the inter-agency review described above, the DNI determined this information falls within an exceptional case wherein the need to protect this information is outweighed by the public interest in the disclosure of this information. *See* Section 3.1(d) of E.O. 13526. Subsequent to the processing of this Order in the Summer of 2013, the IC declassified the fact that there are multiple telecommunications service providers who are directed by FISC orders to provide call detail records as part of this intelligence program. The U.S. Government will provide plaintiff with a new version of this Order with the phrase "those companies" now released.

43. There is also information in this Order that falls within the categories of withholdings that are not being challenged by the plaintiff. This information pertains to the targets of the FBI investigations, the identity of the NSA declarant, and the identity of a FISC employee. This information continues to be properly redacted.

44. The remaining redacted material is still currently and properly classified in accordance with E.O. 13526 or protected from release by statute, specifically, Section 6 of the NSA Act, 50 U.S.C. § 3605, and Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1). This information can be categorized as follows: specific and detailed statistical information that would reveal the scope of the bulk telephony metadata program (p. 2, last paragraph; p. 9, line 3; p. 11, last paragraph (2 places)); the title of the NSA declarant's

organization, the disclosure of which would reveal NSA functions and activities (p. 2, middle); the name of an NSA employee (p.8, FN 4), the redaction of which I understand plaintiff does not challenge; the name of an NSA analytic tool (p. 10, bottom; p. 14 (the two redactions in the body of this page), p. 15 (two redactions)); and information pertaining to an operational technique that NSA was authorized by the FISC to use to query the BR FISA metadata using certain telephone identifiers that were approved for querying (p. 14, FN 6).

45. The statistical information withheld reveals the aggregate number of call detail records that are estimated to be collected by the NSA under Section 215, and this aggregate number remains a currently and properly classified matter in accordance with E.O. 13526. The aggregate amount of call detail records meets the criteria for classification set forth in Sections 1.4(c), 1.4(d), and 1.4(g) of E.O. 13526.

46. I have reviewed this information and determined that the aggregate amount of call detail records is currently and properly classified at the TOP SECRET level in accordance with E.O. 13526, because the release of this information could reasonably be expected to cause exceptionally grave damage to the national security. Additionally, this information is subject to special access and handling restrictions because it involves Sensitive Compartmented Information (“SCI”).⁵ This is so because NSA, pursuant to its SIGINT mission, obtains bulk call detail records from multiple telecommunications service providers, which NSA then queries (term “searches”), pursuant to FISC authorization, to obtain counterterrorism information. Among other benefits, the bulk collection of telephony metadata under Section 215 has an important value to NSA intelligence analysts tasked with identifying potential terrorist threats to

⁵ Sensitive Compartmented Information is “information that not only is classified for national security reasons as Top Secret, Secret, or Confidential, but also is subject to special access and handling requirements because it involves or derives from particularly sensitive intelligence sources and methods.” 28 C.F.R. § 17.18(a).

the U.S. homeland, in support of FBI, by enhancing their ability to detect, prioritize, and track terrorist operatives and their support networks both in the United States and abroad. By applying the FISC-ordered “reasonable, articulable suspicion” (“RAS”) standard⁶ to telephone identifiers used to query the metadata, NSA intelligence analysts are able to: (i) detect domestic identifiers calling foreign identifiers associated with one of the foreign terrorist organizations and discover identifiers that the foreign identifiers are in contact with; (ii) detect foreign identifiers associated with a foreign terrorist organization calling into the United States and discover which domestic identifiers are in contact with the foreign identifiers; and (iii) detect possible terrorist-related communications occurring between communicants located inside the United States.

47. Disclosing the aggregate number of call detail records collected under this program would reveal the scope of this program, the knowledge of which could allow our adversaries to develop countermeasures. Disclosure would also reveal the types of communications that are safe from collection and that are not subject to collection under this program. Disclosing the scope of this program would also allow for possible deduction of the telecommunications service providers who are subject to the FISC orders. With this knowledge, our adversaries could undertake actions to avoid using these telecommunications service providers simply by switching to a provider not subject to these FISC orders, among other steps. Accordingly, any resulting disclosure of this information could reasonably be expected to cause exceptionally grave damage to the national security.

⁶ Before an identifier may be used to query the database, there must be a “reasonable articulable suspicion,” based on factual and practical considerations of everyday life on which reasonable and prudent persons act, that the identifier is associated with one of the identified international terrorist organizations that are subjects of FBI counterterrorism investigations. The U.S. Government recently filed a motion with the FISC that sought, among other things, that (except in emergency cases) the FISC order the U.S. Government to seek the FISC’s permission before the U.S. Government could use a proposed selection term as a “seed” to query the telephony metadata, upon a finding by the FISC that the term to be used satisfies the RAS standard. On February 5, 2014, the FISC granted the U.S. Government’s motion. *In re Application of the FBI for an Order Requiring the Production of Tangible Things from [redacted]*, Dkt. No. BR 14-01 (F.I.S.C. Feb. 5, 2014).

48. This same information is also protected from release by statute and is likewise exempt from release based on FOIA Exemption 3, 5 U.S.C. § 552(b)(3). Specifically, there are two Exemption 3 statutes that protect from public release the identity of any service provider subject to a Primary Order from the FISC: Section 6 of the NSA Act, 50 U.S.C. § 3605, and Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1).

49. The aggregate number of call detail records collected under this authority relates to “any function of the National Security Agency,” 50 U.S.C. § 3605. Indeed, it relates to one of NSA’s primary functions, its SIGINT mission. Further, any disclosure of the scope of this “bulk” collection of call detail records, as stated above, would reveal NSA’s capabilities, particularly given recently declassified information about its abilities to query these call detail records using identifiers. Thus, the aggregate number of call detail records, if revealed, would disclose “information with respect to [NSA’s] activities” in furtherance of its SIGINT mission. 50 U.S.C. § 3605.

50. Likewise, aggregate numbers on the call detail records collected under this program is protected from public release pursuant to Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1), which states that “[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.” Revealing aggregate numbers would provide our adversaries, to include the targets of these FBI investigations, with information from which they could deduce the intelligence sources for the call detail records (the specified service providers), and thus, this information falls squarely within the protection of this statute and afforded absolute protection from release. With this information, our adversaries could attempt to thwart IC activities and undermine the IC’s national security mission.

51. Foreign intelligence targets analyze public disclosures of the IC's capabilities. As such, the public disclosure of either NSA's capability to acquire call detail records or the frequency with which such information is acquired can easily alert targets to the vulnerability of their communications. Also, foreign intelligence targets know how they communicate, and therefore would know, upon a disclosure of NSA's capabilities via the release of the aggregate numbers and any deduction on the likely identities of the specified service providers, which of their call detail records are potentially vulnerable to NSA's collection and querying (and, vice versa, which of their communications may not be vulnerable). Once alerted, targets can frustrate NSA collection by switching to a provider not subject to FISC's Orders. This may result in the denial of access to targets' call detail records and therefore result in a loss of access to information crucial to the national security and defense of the United States.

52. The title of the NSA declarant's organization clearly pertains to a function of the agency and "information with respect to [NSA's] activities" as the title, by itself, reveals specific NSA capabilities and organization, and is thus protected from disclosure based on FOIA Exemption 3 pursuant to Section 6 of the NSA Act.

53. Likewise, the IC withheld the name of an employee as this information is protected from disclosure by Section 6 of the NSA Act, 50 U.S.C. § 3605, and thus exempt from release by FOIA Exemption 3, 5 U.S.C. § 552(b)(3). Section 6 provides, in pertinent part, that "nothing in this Act or any other law...shall be construed to require the disclosure of the organization of any function of the National Security Agency, or any information with respect to the activities thereof, or of the **names**, titles, salaries or number of the persons employed by such agency. (Emphasis added).

54. In this document, the IC also withheld the name of an analytic tool and

information about an operational technique that NSA was authorized by the FISC to use to query the BR FISA metadata using certain telephone identifiers.

55. The information about the operational technique meets the criteria for classification under Sections 1.4(c), 1.4(d), and 1.4(g) of E.O. 13526, and I determined that the fact of this technique, by itself, is currently and properly classified at the TOP SECRET level. Accordingly, this information is exempt from release based on FOIA Exemption 1. This same information likewise falls squarely within Section 6 of the NSA Act, and the National Security Act, and is thus exempt based on FOIA Exemption 3.

56. Disclosure of this specific operational technique that NSA was authorized to use would reveal a specific NSA's technical capability. With this information, our adversaries could attempt to develop countermeasures to frustrate this SIGINT technique. As a result, NSA's ability to maximize the utility of this technique may be significantly hampered. This could reasonably be expected to interfere with the U.S.' gathering of intelligence on its adversaries, including those who may be plotting to harm the United States. Its disclosure therefore could reasonably be expected to cause exceptionally grave damage to the national security of the United States and it is, accordingly, properly classified TOP SECRET pursuant to E.O. 13526.

57. Likewise, the name of the withheld analytic tool clearly relates to a function or activity of the NSA and thus is protected from release by Section 6 of the NSA Act, and exempt under FOIA Exemption 3.

BR 08-13 Supplemental Opinion dated December 12, 2008

58. The only information withheld in this supplemental opinion is the identities of the telecommunications service providers. This information falls within several of the eight enumerated categories of classifiable information set forth in Section 1.4 of E.O. 13526.

Specifically, the identity of any service provider(s) subject to this or any Primary Order falls within Sections 1.4(c), 1.4(d), and 1.4(g) of E.O. 13526.

59. Releasing the identities of any telecommunication service provider subject to any Primary Order would disclose classified intelligence sources, and this would alert the targets of these FBI investigations to which call detail records NSA does and does not collect, as well as the nature and scope of the BR FISA program. With this information, our adversaries would be able to undermine the IC's national security mission.

60. As previously noted, foreign intelligence targets analyze public disclosures of the IC's capabilities. As such, the public disclosure of either NSA's capability to acquire call detail records from certain providers can easily alert targets to the vulnerability of their communications. Also, foreign intelligence targets know how they communicate, and therefore, would know, upon a disclosure of NSA's capabilities via the release of the identity of any particular telecommunications service provider, which of their call detail records are potentially vulnerable to NSA's collection and querying (and, vice versa, which of their communications may not be vulnerable). Once alerted, targets could frustrate NSA collection by switching to a provider not subject to the FISC's Orders. This may result in denial of access to targets' call detail records and therefore result in a loss of access to information crucial to the national security and defense of the United States.

61. This same information is also protected from release by statute and is likewise exempt from release based on FOIA Exemption 3, 5 U.S.C. § 552(b)(3). Specifically, there are two Exemption 3 statutes that protect from public release the identity of any service provider subject to a Primary Order from the FISC: Section 6 of the NSA Act, 50 U.S.C. § 3605, and Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1).

62. The identity of any telecommunications service provider ordered to produce call detail records to the NSA relates to “any function of the National Security Agency,” 50 U.S.C. § 3605. Indeed, it relates to one of NSA’s primary functions, its SIGINT mission. NSA’s SIGINT responsibilities include establishing and operating an effective unified organization to conduct SIGINT activities as set forth in E.O. 12333, section 1.7(c), as amended. In performing its SIGINT mission, NSA exploits foreign electromagnetic signals to obtain intelligence information necessary to the national defense, national security, and the conduct of foreign affairs. NSA has developed a sophisticated worldwide SIGINT collection network that acquires, among other things, foreign and international electronic communications. The technological infrastructure that supports NSA’s foreign intelligence information collection network has taken years to develop at a cost of billions of dollars and untold human effort. It relies on sophisticated collection and processing technology.

63. Pursuant to its SIGINT mission, NSA obtains bulk call detail records from multiple telecommunications service providers identified in FISC Orders, which the NSA, in turn, stores and analyzes under carefully controlled circumstances, and refers to the FBI information about communications (e.g., telephone numbers, dates of calls, etc.) that the NSA concludes have counterterrorism value, typically information about communications between known or suspected terrorist operatives and persons located within the United States.

64. Accordingly, disclosing the identity and participation of the telecommunications service providers would disclose the scope of the “bulk” collection and the communications that are safe and those that are not safe from NSA storage and analysis, as well as information more generally concerning the sources and methods employed by NSA in its mission to collect foreign intelligence. Thus, the identity of the telecommunications service providers, if revealed, would

disclose “information with respect to [NSA’s] activities” in furtherance of its SIGINT mission. 50 U.S.C. § 3605.

65. Likewise, the identities of the specified service providers is protected from public release pursuant to Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1), which states that “[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.” It is without question that the identities of specified service providers in this or any Primary Order are the intelligence sources for the call detail records, and thus, they fall squarely within the protection of this statute and afforded absolute protection from release.

Order Regarding Preliminary Notice of Compliance Incident dated January 28, 2009

66. The IC withheld the following information in this Order: the targets of the FBI investigations, aggregate statistical information on the amount of call detail records to be produced under this program, the NSA declarant’s name, and a FISC employee’s name. Plaintiff is not challenging the withholdings pertaining to targets, the name of the NSA declarant, and the identity of the FISC employee. However, redactions of identities of the telecommunications service providers were already imbedded in the document as found by NSD, as well as the aggregate statistical information about the scope of this program. This information is exempt from release based on FOIA Exemptions 1 and 3 as set forth above, specifically, paragraphs 58-65 for the specified service providers, and paragraphs 45-51 for the statistical information.

Joint PRT/TT [redacted] and BR 09-06 Order and PR/TT [redacted] Supplemental Order⁷

67. This Order and Supplemental Order were treated as one responsive document to

⁷ The justification for the withholdings in this Joint PR/TT and BR order and supplemental PR/TT Order was provided to the plaintiff informally and resulted in the stipulation, wherein plaintiff agreed to not challenge certain categories of withholdings. See FN 1, supra.

the plaintiff's FOIA request, and this document was included twice in the IC's unclassified *Vaughn* index as Documents #048 and #101. Document #048 was reviewed in September 2013 for the September 10, 2013 production, and Document #101 was processed in late October/early November for the November 18, 2013 production.

68. Document #048 was processed through the IC's declassification initiative review process in September 2013. The classification and redaction decisions made while processing Document #048 were made to protect information about the PR/TT bulk metadata program that was properly classified at that time.

69. Due to an administrative error, Document #101 was processed without consideration of the redactions made in Document #048. Further, between the time when Document #048 was processed and Document #101 was processed, the IC made additional declassification decisions. Consequently, in processing this document, the IC released information that was properly classified at the time of initial processing. Unfortunately, because the redactions were not reconciled with the redactions taken in Document #048, the two documents did not contain the same redactions. Upon learning of the inconsistencies, the IC reconciled the redactions and released a revised version of this Order on November 18, 2013, wherein all information released in #048 and #101 was released. This declaration discusses the withholdings contained in the version of this Order released on November 18, 2013.

70. In this Order, the identities of the targets of these investigations, the identities of the telecommunications service providers, and the identity of the NSA declarant have been withheld. The justification for withholding the identities of the telecommunications service providers are set forth above at paragraphs 58-65. Additionally, certain operational details about the PR/TT program have been withheld based on FOIA Exemptions 1 and 3. These details

include the docket numbers, which are found throughout this document, dates (found throughout the document), and the number of reports identified in the NSA declaration (page 3).

71. These operational details were protected so that our Nation's adversaries could not deduce any gaps in coverage that occurred when this program was operational. By revealing the docket numbers for this PR/TT program and dates, which comprise the majority of withholdings in this document, our adversaries could deduce or infer the time period for which the program was not operational, thereby determining which of their communications (email metadata) may have escaped NSA collection and querying. This information meets the criteria for classification in Sections 1.4(c), 1.4(d), and 1.4(g) of E.O. 13526 and is currently and properly classified at the TOP SECRET level. Likewise, this information relates to a function or an activity of the NSA, specifically its SIGINT mission, and the activities carried out in furtherance of this mission with this particular intelligence program.

72. Regarding the IC's withholding of the number of reports generated from this PR/TT program, this information was initially protected as it revealed NSA capabilities with this program in determining the connections between known and unknown international terrorist operatives. The number of reports can now be released, not based on this current litigation, but based on the President's transparency initiative. This piece of information meets the criteria for classification, however, after the inter-agency review described above, the DNI determined this information falls within an exceptional case wherein the need to protect this information is outweighed by the public interest in the disclosure of this information. *See* Section 3.1(d) of E.O. 13526. The U.S. Government will provide plaintiff with a new version of this Order with the number of PRTT reports now released.

73. The PR/TT [] Supplemental Order does not contain a significant legal

interpretation of Section 215, or interpret Section 215 at all. It is therefore not responsive to plaintiff's FOIA request that is the subject of this litigation, but was released to plaintiff and to the public in the discretion of the U.S. Government. In that release, NSA withheld docket numbers and dates for the reasons set forth in ¶ 71 above; the name of the same database withheld in BR 09-13 Primary Order for the reasons set forth in ¶ 90 below; and the name of an NSA declarant, which is not being challenged by the plaintiff. In releasing this Supplemental Order, NSA initially withheld information that describes identifiers utilized as part of its defeat list. This information is NSA's use of "high volume" selectors, and it was declassified in recent Primary Orders, not based on this current litigation or any other litigation, but based on the President's transparency initiative and requests by the FISC to declassify current Primary Orders among other Orders. *See* BR 14-01 Primary Order, dated January 3, 2014, on the icontherecord.tumblr.com website at the February 12, 2014 Joint Statement by the DNI and AG. The U.S. Government will provide plaintiff with an updated version of this Supplemental Order with the term "high volume" released as found in the Supplemental Order.

BR 09-13 Primary Order⁸ and Secondary Orders⁹

74. This Primary Order, which was issued by the FISC pursuant to the BR provision of the FISA, 50 U.S.C. § 1861, enacted by Section 215, granted the U.S. Government's application for production of certain call detail records finding "reasonable grounds to believe that the [records] sought are relevant to authorized investigations ...being conducted by the FBI

⁸ The justifications for the IC's withholdings in this Primary Order were also provided to the plaintiff informally. Since some of the withholdings in this document are still being challenged, the U.S. Government is again providing the justification for the withholdings of the still challenged information.

⁹ All Secondary Orders have been withheld in their entirety as any attempt to redact the identity of the service providers in these Secondary Orders, in compilation with other documents that have been declassified, i.e., the BR 13-80 Primary Order and Verizon Secondary Order, would allow a reader to ascertain the identity of the provider simply by looking at the size of the redacted/blocked material, or comparing any redacted Secondary Order with other declassified documents.

... to protect against terrorism.” *In re Application of the FBI for an Order Requiring the Production of Tangible Things [etc.]*, Dkt. No. BR 09-13, Primary Order at 1-2 (F.I.S.C. Sep. 03, 2009).

75. This Primary Order directed the daily production to NSA of electronic copies of “all call detail records, or ‘telephony metadata,’” created by a recipient telecommunications service provider for calls to, from, or wholly within the United States. BR 09-13 Primary Order at 3-4. *See also*, BR 13-80 Primary Order at 3-4; BR 13-80 Secondary Order at 1-2.

76. Within the BR 09-13 Primary Order, the IC withheld the following categories of information: identities of the telecommunications service providers subject to the FISC’s order; the target(s) of FBI’s investigations; the identity of NSA’s declarant whose declaration in support of the U.S. Government’s application is referenced in this Order; operational details about telephone identifiers and an intelligence technique; operational details about intelligence sources; an operational detail relating to how NSA receives the BR metadata from a specified service provider; the name of an NSA intelligence database; and the identity of a FISC employee/clerk. As stated above, plaintiff is not challenging the withholdings pertaining to the targets of FBI investigations; identities of U.S. Government declarants; operational details about intelligences sources and the FISC’s treatment of call detail records from such sources; operational detail disclosing how the NSA obtains metadata from a specified service provider or providers; and the identities of FISC or other U.S. Government employees withheld pursuant to FOIA Exemptions 6 and 7(C).

77. Plaintiff does challenge the withholding of the identities of the telecommunications service providers that were ordered to produce call detail records to the NSA pursuant to this Primary Order. This information, however, is a currently and properly

classified matter in accordance with E.O. 13526 and thus exempt from release pursuant to FOIA Exemption 1. This information falls within several of the eight enumerated categories of classifiable information set forth in Section 1.4 of E.O. 13526. Specifically, the identity of any service provider(s) subject to this or any Primary Order falls within Sections 1.4(c) and 1.4(g) of E.O. 13526.

78. I reviewed this information and determined that the identity of the service providers in this BR 09-13 Primary Order is currently and properly classified at the TOP SECRET level in accordance with E.O. 13526, because the release of this information could reasonably be expected to cause exceptionally grave damage to the national security. Additionally, this information is subject to special access and handling restrictions because it involves SCI.

79. This same information is also protected from release by statutes and is likewise exempt from release based on FOIA Exemption 3, 5 U.S.C. § 552(b)(3). Specifically, there are two Exemption 3 statutes that protect from public release the identity of any service provider subject to a Primary Order from the FISC: Section 6 of the NSA Act, 50 U.S.C. § 3605, and Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1).

80. The identity of any company ordered to provide call detail records to the NSA clearly relates to “any function of the National Security Agency,” 50 U.S.C. § 3605. Indeed, it relates to one of NSA’s primary functions, its SIGINT mission. NSA’s SIGINT responsibilities include establishing and operating an effective unified organization to conduct SIGINT activities as set forth in E.O. 12333, section 1.7(c), as amended. In performing its SIGINT mission, NSA exploits foreign electromagnetic signals to obtain intelligence information necessary to the national defense, national security, and the conduct of foreign affairs. NSA has developed a

sophisticated worldwide SIGINT collection network that acquires, among other things, foreign and international electronic communications. The technological infrastructure that supports NSA's foreign intelligence information collection network has taken years to develop at a cost of billions of dollars and untold human effort. It relies on sophisticated collection and processing technology.

81. Pursuant to its SIGINT mission, and as authorized by the FISC, NSA quickly analyzes past connections and chains of communication through telephony metadata collected pursuant to Section 215. Unless the data is aggregated, it may not be feasible to detect chains of communications that cross communication networks. The ability to query accumulated telephony metadata significantly increases the NSA's ability to rapidly detect persons affiliated with the identified foreign terrorist organizations who might otherwise go undetected.

82. Accordingly, disclosing the identities of the telecommunications service providers would disclose the scope of the "bulk" collection and reveal much about NSA's capabilities in determining the connections between known and unknown international terrorist operatives across different providers as part of these authorized investigations under Section 215, as well as the sources and methods used by the NSA in conducting its foreign intelligence mission. Thus, the identities of the telecommunications service providers, if revealed, would disclose "information with respect to [NSA's] activities" in furtherance of its SIGINT mission. 50 U.S.C. § 3605.

83. Likewise, the identities of the telecommunications service providers is protected from public release pursuant to Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1), which states that "[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure." It is without question that the

identities of specified service providers in this or any Primary Order are the intelligence sources for the call detail records, and thus, they fall squarely within the protection of this statute and afforded absolute protection from release.

84. Releasing the identities of any telecommunications service provider subject to any Primary Order would disclose classified intelligence sources, and this would alert the targets of these FBI investigations to which call detail records NSA does and does not collect, as well as the nature and scope of the BR FISA program. With this information, our adversaries could attempt to undermine the IC's national security mission.

85. Foreign intelligence targets analyze public disclosures of NSA's capabilities. As such, the public disclosure of either NSA's capability to acquire call detail records or the frequency with which such information is acquired can easily alert targets to the vulnerability of their communications. Also, foreign intelligence targets know how they communicate, and therefore, would know, upon a disclosure of NSA's capabilities via the release of the identity of any particular telecommunications service provider, which of their call detail records are potentially vulnerable to NSA's collection and querying (and, vice versa, which of their communications may not be vulnerable). Once alerted, targets can frustrate NSA collection by switching to a provider not subject to this or any other Primary Order. This may result in denial of access to targets' call detail records and therefore result in a loss of access to information crucial to the national security and defense of the United States.

86. The withholdings under this category of information can be found in this Primary Order on pages 1 (case caption), 3, 4, and 11.

87. The IC withheld information that pertains to an operational technique that NSA was authorized by the FISC to use to query the BR FISA metadata using certain telephone

identifiers that were approved for querying, and information that describes “telephone identifiers.” This information meets the criteria for classification under Sections 1.4(c) and 1.4(g) of E.O. 13526 and as an OCA, I determined that the fact of this technique, by itself, is currently and properly classified at the TOP SECRET level. Accordingly, this information is exempt from release based on FOIA Exemption 1. This same information likewise falls squarely within Section 6 of the NSA Act and the National Security Act, and is thus exempt based on FOIA Exemption 3.

88. Disclosure of this specific operational technique that NSA was authorized to use would reveal to our adversaries NSA’s technical capabilities. With this information, our adversaries could attempt to develop countermeasures to frustrate this SIGINT technique. As a result, NSA’s ability to maximize the utility of this technique may be significantly hampered.

89. Any releases of the description of “telephone identifiers” would reveal to our adversaries highly detailed facts about the nature of the NSA’s uses of a specific intelligence source that could assist them in undermining the IC’s national security mission. Again, foreign intelligence targets know how they communicate, and upon a disclosure of information that describes the telephone identifiers used by NSA, these targets would know what type of information NSA collects (and vice versa, the type of information NSA does not collect). With this information, targets will attempt to frustrate NSA’s collection of their call detail records and/or NSA’s ability to query using such information. The information in this category can be found at page 6, to include footnote 2, and at page 15.

90. The name of the NSA database relates to a function or activity of the NSA, and thus falls squarely within the protections afforded by Section 6 of the NSA Act. Accordingly, the name of this database, particularly given the official release of its description (it stores BR

FISA metadata) as revealed in this document, is exempt from release based on FOIA Exemption 3 based on compilation. This is so because any release of the database name may provide a foreign intelligence service with information that would be useful should they attempt to penetrate NSA networks. When reviewing this information, the U.S. Government was faced with two choices—release the name of the database but protect details or release details about the database, but protect the name. The U.S. Government chose the latter as it provides additional information and is consistent with the spirit of the FOIA. This information can be found at page 12.

BR 09-13 Order Regarding Further Compliance Incidents dated September 25, 2009

91. The only information withheld by the IC in this opinion is the identities of the specified service providers, targets of FBI investigations (no longer challenged by plaintiff), the name of an FBI investigation, and the name of the FISC employee (no longer challenged by plaintiff). The only withholding being challenged in this Order is the identity of the telecommunications service providers, which was justified above.

BR 09-15 Supplemental Opinion and Order dated November 5, 2009

92. The only information withheld by the IC in this opinion is the aggregate number of call detail records that are estimated to be collected by the NSA under Section 215, which is classified as discussed above at ¶¶ 45-51, and the identities of the service providers, which is classified as discussed above at ¶¶ 58-65. All other withheld material consists of information not challenged by plaintiff: the identities of the targets of FBI investigations, the name of an FBI investigation, the name of the NSA declarant, and the name of the FISC employee.

FISC Supplemental Order BR 10-82 dated November 23, 2010

93. A FISC Supplemental Order in BR 10-82, dated November 23, 2010 and consisting of two pages, has been withheld in part to protect certain classified and law enforcement sensitive information. The case underlying BR 10-82 is an FBI counterterrorism investigation of a specific target. That investigation is still pending. Here, in the course of a pending counterterrorism investigation, the FBI sought authorization under the FISA to obtain financial records, under the FISA's business records provision, pertaining to the target of the investigation and in fact obtained such authorization. What follows is the justification for withholding the last paragraph of the order pursuant to FOIA Exemption 7(A).

94. Exemption 7(A) protects "records or information compiled for law enforcement purposes [when disclosure] could reasonably be expected to interfere with enforcement proceedings." 5 U.S.C. § 552(b)(7)(A). Application of Exemption 7(A) requires: the existence of law enforcement records; a pending or prospective law enforcement proceeding; and a determination that release of the information could reasonably be expected to interfere with the enforcement proceeding. Courts afford deference to agencies' predictive judgments of harm to pending enforcement proceedings, particularly in the national security context. Here, in the course of a pending counterterrorism investigation, the FBI sought authorization under the FISA to obtain certain financial records. This FISC Supplemental Order, which was issued in relation to its authorization for such collection, was thus compiled for law enforcement purposes, in furtherance of a national security investigation within the FBI's authorized law enforcement duties. Accordingly, this Supplemental Order readily satisfies Exemption 7's threshold requirement.

95. The remaining inquiry is whether disclosure of information from this Supplemental Order could reasonably be expected to interfere with enforcement proceedings –

i.e., the FBI's pending investigation and/or any resulting prosecutions. Here, the FBI has determined that the release of the final paragraph of the order, which describes certain requirements reflecting the FBI's particular implementation of the authority granted by the FISC, could reasonably be expected to adversely impact the pending investigation and any resulting prosecutions. Release of this paragraph would reveal the specific and unique implementation requirements imposed on the FBI under this FISA-authorized collection during a particular time period. It is unclear what and how much the target might already know about the FBI's investigation. However, as more fully explained in my classified, *ex parte, in camera* declaration, there is reason to believe that the target or others knowledgeable about the nature and timing of the investigation could piece together this information, the docket number, the dates of the collection, and other information which has already been released or deduced to assemble a picture that would reveal to the target that the target was the subject of a particular type of intelligence collection during a specific time period, and by extension, that the target's associates during that period may have been subject to similar intelligence collections. This could lead the target to deduce the scope, focus, and direction of the FBI's investigative efforts, and potentially any gaps in the collections, from which the target could deduce times when the target's activities were "safe." Thus, disclosure could reasonably be expected to adversely affect the FBI's investigation by arming the target and others with information that could be used to circumvent continuing investigative efforts, develop countermeasures, and otherwise attempt to elude further detection. For example, if the target deduced that the FBI was obtaining the target's and the target's associates' financial information from a particular entity, the target could change banks or otherwise modify the target's behavior to elude such scrutiny, thus impeding a valuable avenue of information in this investigation. Any information that tipped the target off

to particular FBI scrutiny could reasonably be expected to result in evasive actions by the target in an attempt to thwart the FBI's investigation. Moreover, it could also reasonably be expected to adversely affect any resulting prosecutions by providing access to investigation information that may become pertinent to the prosecution and by revealing information that could provide insights into the prosecutors' strategy and the strength of the government's position.

96. The November 23, 2010 FISC Supplemental Order in BR 10-82 has been carefully reviewed to determine whether there was any reasonably segregable, non-exempt information that could be released to plaintiff, in compliance with the FOIA's segregability provision, 5 U.S.C. § 552(b). This segregability determination was also made in light of the principle that agencies are not required to segregate and release segments of information that, if disclosed, would lack meaning. Based on a thorough review of the Supplemental Order, it was determined that the document could be released in part, with only the identity of the entity from which information was collected and the particular implementation requirements described in the final paragraph being redacted. As to that final paragraph, however, there is no reasonably segregable information that can be released. Specifically, all exempt information is either inextricably intertwined with any non-exempt information or the non-exempt information would, if excised and released, lack meaning on its own. Accordingly, no further information can be redacted and released from this document without disclosing exempt information.

D. WITHHELD IN FULL FISC BR 08-07

97. In this unclassified declaration, I am also able to address the justification for withholding in full the FISC BR 08-07 Supplemental Opinion, dated August 20, 2008, because the facts justifying the withholdings in this document are not themselves indicative of still classified intelligence sources, methods, and activities. As discussed further below, the

withholdings in this document are made pursuant to FOIA Exemptions 1 and 3 and there is no meaningful, non-exempt information that can be segregated from the exempt information.

98. The FISC BR 08-07 Supplemental Opinion addresses the NSA's use of a specific intelligence method in the conduct of queries (term "searches") of telephony metadata or call detail records obtained pursuant to the FISC's orders under the BR FISA program and was thus withheld in full. The opinion is only six pages in length and the specific intelligence method is discussed at great length in every paragraph of this opinion, including in the title. Upon review of this opinion, I have determined that there is no meaningful, segregable, non-exempt information that can be released to the plaintiff as the entire opinion focuses on this intelligence method. Even if the name of the intelligence method was redacted, the method itself could be deduced, given other information that the DNI has declassified pursuant to the President's transparency initiative and the sophistication of our Nation's adversaries and foreign intelligence services.

99. Thus, the entire opinion is currently and properly classified TOP SECRET based on the procedure of classification by compilation.¹⁰ *See* E.O. 13526, Section 1.7(e) ("Compilation of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that: (1) meets the standard for classification under this order; and (2) is not otherwise revealed in the individual items of information."). Accordingly, as the Supreme Court has recognized, "bits and pieces of data may aid in piecing together bits of other information even when the individual piece is not of obvious importance in itself. . . . Thus, what may seem trivial to the uninformed, may appear

¹⁰ Even the case caption is exempt as it identifies the telecommunications service providers who are ordered to produce call detail records and the targets of FBI investigations. The only information that could be releasable is the docket number BR 08-07, which is not meaningful as it does not provide any information to the plaintiff on what the order pertains to beyond what the IC has already indicated at the beginning of this case—it is a document responsive to the plaintiff's FOIA request.

of great moment to one who has a broader view of the scene and may put the questioned item of information in its proper context.” *See CIA v. Sims*, 471 U.S. 159, 178 (1985) (internal quotations and citations omitted)).

100. Based on compilation, the information in this opinion, if disclosed, would reveal an intelligence method that is used in various intelligence activities and accordingly, this information meets the criteria for classification under Sections 1.4(c), 1.4(d), and 1.4(g) of E.O. 13526, and is in fact currently and properly classified TOP SECRET. Thus, all of the information in this opinion is exempt from release based on FOIA Exemption 1.

101. The intelligence method discussed in this opinion is also protected from public release pursuant to Section 6 of the NSA Act because the intelligence method pertains to a function of the NSA, in fact, one of its most important functions, its SIGINT mission, and activities undertaken to carry out its SIGINT mission. Accordingly, this same information, because it relates to an intelligence method, is protected from release pursuant to the National Security Act, as amended, 50 U.S.C. § 3024(i)(1).

102. This intelligence method is used to conduct queries of the bulk metadata, and if NSA were no longer able to use this method because it had been compromised, NSA’s ability to analyze bulk metadata would itself be compromised. A lost or reduced ability to detect communications chains that link to identifiers associated with known and suspected terrorist operatives, which can lead to the identification of previously unknown persons of interest in support of anti-terrorism efforts both within the United States and abroad, would greatly impact the effectiveness of this program as there is no way to know in advance which numbers will be responsive to the authorized queries. Further, any disclosure of this intelligence method may allow our adversaries to undertake countermeasures to degrade the effectiveness of NSA’s

querying of the bulk metadata using this intelligence method. The countermeasures cannot be discussed in a public declaration without revealing the very information that the IC is protecting from release pursuant to FOIA Exemptions 1 and 3--this intelligence method.

103. I cannot provide further explanation of the classification of this intelligence method on the public record without risking disclosure of classified information. In the event the Court requires a more detailed discussion of the harm to the national security should this intelligence method be disclosed, and a further explanation of why such disclosure could reasonably be expected to occur if this opinion were to be released, even in part, the U.S. Government will provide such further, classified detail in an *ex parte* submission for the Court's *in camera* consideration.

104. As indicated above, the U.S. Government's withholdings in this case were appropriate and consistent with the FOIA's requirements under the circumstances. All of the withholdings of NSA information in these documents can be justified based on Exemption 3 alone pursuant to Section 6 of the NSA Act as the withheld information relates to "any function" of the NSA and "information with respect to [NSA's] activities" in furtherance of its SIGINT mission. Further, all of the withheld information is likewise exempt based on FOIA Exemption 1.

E. REMAINING ORDERS WITHHELD IN FULL

105. The scope of the IC declassification initiative has been substantial and has required a diligent and arduous balancing of the public interest in an informed public discussion and the harm to national security that could result from providing information to U.S. adversaries that could permit them to identify U.S. intelligence capabilities and take steps to evade detection and collection. As stated above, one of the greatest challenges the United States faces in

combating international terrorism is identifying terrorist operatives and the threats they pose. The IC declassification initiative has necessarily been limited to ensure these and other adversaries are not given the means by which to evade such detection. Therefore, although the IC declassification initiative has permitted significant unclassified details to be provided regarding the justifications for the withholdings in many of the documents that are currently at issue in this case, certain information regarding specific withholdings can only be explained in a classified declaration. Here, to the extent possible, I will provide an unclassified explanation of those withholdings.

106. The remaining FISC Orders have been withheld in full pursuant to FOIA Exemptions 1, 3, and 7(E), 5 U.S.C. §§ 552(b)(1), (3), and (7)(E). I have determined, in consultation with IC officials, that the U.S. Government cannot publicly disclose further details about the contents of these documents, which remain currently and properly classified in accordance with E.O. 13526, without revealing classified information, information that is protected from release by statute (*i.e.*, the National Security Act), and/or information that is properly exempt from disclosure pursuant to FOIA Exemption 7(E). These FISC Orders, which are classified at the SECRET level, meet the substantive requirements of E.O. 13526 § 1.1(a) because: (1) the information was classified by an OCA; (2) is owned by, produced by or for, or is under control of the U.S. Government; (3) falls within § 1.4(c) of E.O. 13526; and (4) the OCA determined that unauthorized disclosure of the information reasonably could be expected to result in serious damage to the national security. A description of that damage is set forth below. Additionally, the applicable procedural requirements for classifying information set forth in E.O. 13526 were followed.

107. These remaining FISC Orders are being withheld in full in order to protect information about intelligence methods utilized by the IC for gathering intelligence data. This material was classified to protect from disclosure information that would reveal actual intelligence sources, activities, and methods used against targets and to protect the intelligence-gathering capabilities of the activities or methods. Disclosure of information describing the intelligence activities or methods that were used and that are still used to gather intelligence information in other cases could reasonably be expected to cause serious damage to the national security for the following reasons. The FISC Orders specifically describe how the IC technically and operationally implements its FISA authorities. Moreover, they identify the types of information being collected and the dates of collection. Disclosure of this information would allow targets to know what information the IC was collecting at particular times, as well as gaps in coverage that would reveal that information from a particular period was “safe.” Consequently, the IC’s intelligence-gathering capabilities would be severely disrupted and result in severe damage to efforts to detect and apprehend violators of the U.S.’ national security and criminal laws if this information were to be disclosed. Because disclosure of this information could reasonably be expected to cause serious damage to the national security, it is properly classified at the SECRET level and withheld pursuant to E.O. 13526 § 1.4(c) and is exempt from disclosure under FOIA Exemption 1.

108. Docket numbers have also been protected from disclosure as they would reveal that the U.S. Government is utilizing a specific FISA-authorized technique on the subject, which is considered a classified technique and method. In conjunction with the dates of the Orders, which have already been disclosed to the plaintiff, this information would provide targets with information concerning the duration of the collection. This additional information, together with

other information, would show the extent and duration of the use of this particular, currently-used and classified technique. Adversarial intelligence services and hostile entities search continually for information regarding the activities of the IC and are able to gather information from myriad sources. Providing an additional piece of information regarding the specific FISA-authorized techniques and methods utilized at particular times by the IC – which would reveal the types of information being collected as well as the types not being collected – could allow these entities to analyze this and other information, and devise ways to circumvent and defeat IC activities from seemingly disparate pieces of information. Accordingly, revelation of this information could allow the U.S.' adversaries to piece together detailed pictures of the IC's use of this currently-utilized, classified technique in order to circumvent or thwart it. Thus, disclosure of this information could reasonably be expected to cause serious damage to the national security and accordingly it is currently and properly classified at the SECRET level, protected pursuant to E.O. 13526 § 1.4(c), and withheld under FOIA Exemption 1.

109. The information withheld in this case pursuant to Exemption 1, including information in these documents that are withheld in full, was examined in light of the body of information available to me concerning the national defense and foreign relations of the United States. This information was not examined in isolation. Instead, it was evaluated with careful consideration given to the impact that its disclosure will have on other sensitive information contained elsewhere in the IC's files. Equal consideration was given to the impact that other information either in the public domain or likely known or suspected by present or potential adversaries of the United States would have upon the information I examined.

110. The justifications for the withheld classified information were prepared with the intent that they be read with consideration given to the context in which the classified

information is found. This context includes any surrounding unclassified information, other information already in the public domain, and information likely known or suspected by other hostile intelligence entities. Any greater specificity in the descriptions and justifications set forth with respect to information relating to intelligence activities and methods of the United States could reasonably be expected to jeopardize the national security of the United States.

111. FOIA Exemption 3 was also asserted to withhold these FISC Orders pursuant to Section 102A(i)(1) of the National Security Act, as amended, 50 U.S.C. § 3024(i)(1). On its face, this federal statute leaves no discretion about withholding from the public information about intelligence sources and methods. Thus, the protection afforded to intelligence sources and methods by 50 U.S.C. § 3024(i)(1) is absolute. In order to fulfill his obligation of protecting intelligence sources and methods, the DNI is authorized to establish and implement guidelines for the IC for the classification of information under applicable laws, Executive orders, or other Presidential directives, and for access to and dissemination of intelligence. 50 U.S.C. §§ 3024(i)(2)(A), (B).

112. As described above, Congress enacted section 3024(i) of the National Security Act, as amended, to protect the IC's sources and methods of gathering intelligence. Disclosure of such information presents the potential for individuals and organizations to develop and implement countermeasures, which would result in the loss of significant intelligence information relied upon by national policymakers and the IC. Details about specific intelligence-gathering methods used by the IC would be revealed if any of the withheld information is disclosed to the plaintiff. Accordingly, this information was properly withheld pursuant to FOIA Exemption 3 based on 50 U.S.C. § 3024(i)(1).

113. Additionally, information in these documents was withheld pursuant to FOIA Exemption 7(E), which exempts from disclosure:

records or information compiled for law enforcement purposes, but only to the extent that production of such law enforcement records or information ... would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

5 U.S.C. § 552(b)(7)(E).

114. Exemption 7's threshold requirement is met because the information was compiled for a law enforcement purpose. Exemption 7(E) has been asserted in order to protect non-public details about the IC's use of a law enforcement technique in furtherance of national security investigations. Details about how, when, and under what circumstances these techniques are relied upon in the context of national security investigations are not disclosed nor are these details otherwise known to the public. Disclosure of such information could enable individuals and organizations to circumvent the use of the technique, and the relative benefit of the technique could be diminished if details about its particular use were revealed here. This, in turn, could facilitate the accumulation of information by subjects of on-going investigations regarding the circumstances under which the technique was used, the usefulness of the technique in particular types of investigations, and the value of the information obtained. Release of this type of information could enable subjects of investigations to educate themselves about the use of this technique in particular to locate and apprehend individuals and gather and analyze evidence. This would allow individuals and organizations to take countermeasures to circumvent or negate the effectiveness of the technique. Thus, the U.S. Government has properly protected some of the information at issue from disclosure pursuant to FOIA Exemption

7(E). Further details about the technique cannot be disclosed publicly without revealing the very information exempted from disclosure by Exemption 7(E).

V. SEGREGABILITY

115. All of these documents have been reviewed for purposes of complying with FOIA's segregability provision which requires the U.S. Government to release "any reasonably segregable portion of a record" after proper application of the FOIA exemptions. 5 U.S.C. § 552(b). An intensive, line-by-line review of each one of these documents was performed by multiple agencies and all reasonably segregable, non-exempt information has been released.

116. This pertains to even otherwise unclassified information that is contained in the withheld in full documents, including legal analysis. The legal analysis in the withheld in full documents cannot reasonably be segregated and released without risking disclosure of currently and properly classified information concerning the manner and means by which the United States acquires tangible things for certain authorized investigations pursuant to Section 215.

117. Further, with respect to the withheld in full FISC opinions and orders, it is my judgment that any information in those documents that, viewed in isolation, could be considered unclassified, is nonetheless classified in the context of this case because it can reasonably be expected to reveal (directly or by implication) classified national security information concerning the timing or nature of intelligence activities, sources and methods when combined with other information that might be available to the public or adversaries of the United States. In these circumstances, the disclosure of even seemingly mundane portions of these FISC opinions or orders, when considered in conjunction with other publicly available information, could reasonably be expected to assist a sophisticated adversary in deducing particular intelligence activities or sources and methods, and possibly lead to the use of countermeasures that may

deprive the United States of critical intelligence.

118. Thus, for example, it is my judgment that, although certain legal analysis set forth in the withheld in full FISC opinions may be unclassified when viewed in isolation, it is not reasonably segregable here because, when viewed in the context of this FOIA request and other public information, it would tend to reveal information about classified intelligence sources, methods, and activities at issue in the balance of the document. In particular, legal analysis would tend to reveal how statutory and judicial authority are being applied in a specific context to the use or application of a particular intelligence source and method. Therefore, while it is unclassified that the FISA authorizes the United States to acquire tangible things for certain authorized investigations pursuant to Section 215, and it is now unclassified that the United States collects telephony metadata in bulk pursuant to this authority under supervision of the FISC, the documents that remain withheld in full following the inter-agency review and extensive declassification initiative described above cannot be reasonably segregated because they would reveal further specific information about intelligence sources and methods that remains properly classified.

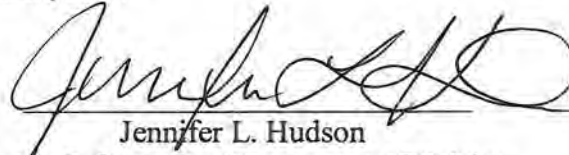
119. Finally, I have also determined that providing further information regarding the particular dates of some of the FISC opinions withheld in full would also tend to reveal classified information. In my judgment, providing additional date information beyond a date range would tend to reveal non-public information about when the U.S. Government was or was not using its authorities under Section 215. When combined with information that is public or otherwise already known to adversaries of the United States, such information could be used to extrapolate how and when the U.S. Government has used certain intelligence sources and methods under Section 215, and to correlate the use of Section 215 authority to certain events that may be public

or otherwise known to adversaries of the United States. Accordingly, I have determined that the disclosure of further information as to the specific dates of one of these FISC opinions could tend to reveal information concerning still-classified details regarding intelligence collection methods and could reasonably be expected to cause exceptionally grave damage to, *inter alia*, national security.

CONCLUSION

I certify under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Executed this 28th day of March, 2014

A handwritten signature in black ink, appearing to read "Jennifer L. Hudson", written over a horizontal line.

Jennifer L. Hudson
Director, Information Management Division
Office of the Director of National Intelligence