

EXHIBIT B

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

ELECTRONIC FRONTIER FOUNDATION,)	Case No.: 14-cv-03010-RS
)	
Plaintiff,)	
)	
v.)	
)	
NATIONAL SECURITY AGENCY, OFFICE)	
OF THE DIRECTOR OF NATIONAL)	
INTELLIGENCE,)	
)	
)	
Defendants.)	

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. In my current position, I am the final decision-making authority for the ODNI/IMD.

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

1 management and declassification, pre-publication reviews, and responding to requests under the
2 Freedom of Information Act (“FOIA”) and the Privacy Act.

3 3. Under a written delegation of authority by the Director of National Intelligence
4 (“DNI”) pursuant to section 1.3(c) of Executive Order 13526, I hold original classification
5 authority (“OCA”) at the TOP SECRET level. I am authorized, therefore, to conduct classification
6 reviews and to make original classification and declassification decisions for intelligence
7 information up to and including the TOP SECRET level.

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

11 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
12 and justify, to the extent possible on the public record, the actions taken by the Intelligence
13 Community (“IC”) in responding to plaintiff’s request for information under the FOIA, 5 U.S.C. §
14 552.
15

16 **I. ODNI BACKGROUND**

17 6. Congress created the position of the DNI in the Intelligence Reform and Terrorism
18 Prevention Act of 2004, Pub. L. No. 108-458, §§ 1101(a) and 1097, 118 Stat. 3638, 3643-63, 3698-
19 99 (2004) (amending Sections 102 through 104 of Title 1 of the National Security Act of 1947).
20 Subject to the authority, direction, and control of the President, the DNI serves as the head of the
21 IC and as the principal adviser to the President and the National Security Council for intelligence
22 matters related to the national security. 50 U.S.C. §§ 3023(b)(1), (2).

23 7. The responsibilities and authorities of the DNI are set forth in the National Security
24 Act of 1947, as amended. These responsibilities include ensuring that national intelligence is
25 provided to the President, heads of the departments and agencies of the Executive Branch, the
26 Chairman of the Joint Chiefs of Staff and senior military commanders, and the Senate and House
27 of Representatives and committees thereof. 50 U.S.C. § 3024(a)(1). The DNI is charged with
28 establishing the objectives of; determining the requirements and priorities for, and managing and

1 directing the tasking, collection, analysis, production, and dissemination of national intelligence by
2 elements of the IC. 50 U.S.C. §§ 3024(f)(1)(A)(i) and (ii).

3 8. In addition, the National Security Act of 1947, as amended, provides that the DNI
4 “shall protect intelligence sources and methods from unauthorized disclosure.” 50 U.S.C. §
5 3024(i)(1). Consistent with this responsibility, the DNI establishes and implements guidelines for
6 the IC for the classification of information under applicable law, executive orders, or other
7 presidential directives, and for access to and dissemination of intelligence. 50 U.S.C. §
8 3024(i)(2)(A), (B).

9 9. The function of the ODNI is to assist the DNI in carrying out his duties and
10 responsibilities under the Act and other applicable provisions of law, and to carry out such other
11 duties as may be prescribed by the President or by law.

12 **II. PLAINTIFF’S FOIA REQUEST**

13 10. By letter dated May 6, 2014, the requester Electronic Frontier Foundation submitted
14 a request under the FOIA. The requester requested the following:

15 All records, emails and communications related to the development or
16 implementation of the “Vulnerabilities Equity Process” and all records, emails and
17 communications related to or reflecting the “principles” that guide the agency
18 “decision-making process for vulnerability disclosure” in the process described in
19 the White House blog post.

20 11. In order to satisfy any FOIA request, the IMD must locate information that is
21 responsive to the request within ODNI systems of records.

22 12. As part of this process, IMD identifies, within ODNI systems of records, those
23 records or portions of records that originated with other agencies or that implicate the equities of
24 other agencies. The IMD then sends a consultation request to those agencies, along with those
25 identified records. The purpose of the consultation request is to secure the assistance of those
26 agencies in ascertaining whether information contained within those documents is responsive to
27 the request and appropriate for release under the FOIA.

28 13. In this case IMD identified thirteen (13) different agencies whose equities were
represented in the documents and sent consultation requests to those agencies.

1 14. Prior to the ODNI's receiving responses to all the consultation requests, the plaintiff
2 filed suit to compel production of the documents requested in its May 6, 2014 FOIA request. That
3 suit was filed on July 1, 2014.

4 15. It is my understanding that on October 22, 2014, the court entered an order staying
5 the proceedings until April 20, 2015 and set forth a production schedule as follows:

- 6 • December 15, 2014: Defendant Office of the Director of National Intelligence (ODNI)
7 will complete processing responsive documents that originated with ODNI (and do not
8 require outside consultation) and produce non-exempt, responsive information.
- 9 • January 15, 2015: Defendant ODNI will produce non-exempt, responsive information
10 from documents that require consultation completed as of that date.
- 11 • March 25, 2015: Defendant ODNI will complete processing the remaining documents
12 that require consultation and produce non-exempt, responsive information.¹

13 16. On December 15, 2014, ODNI sent a response letter to the plaintiff. In that letter
14 ODNI informed the plaintiff that it had located six (6) documents that contained information that
15 was responsive to the request. The letter further informed plaintiff that it was releasing three (3) of
16 those documents in segregable form with deletions made pursuant to FOIA exemptions (b)(1),
17 (b)(3), (b)(5), and (b)(6), and that three (3) additional responsive documents were being withheld
18 in full pursuant to FOIA exemptions (b)(1), (b)(3), and (b)(5).

19 17. On January 15, 2015, ODNI sent a response letter to the plaintiff. In that letter
20 ODNI informed the plaintiff that it had located eight (8) documents that contained information that
21 was responsive to the request but that it was withholding the documents in their entirety pursuant
22 to FOIA exemptions (b)(1), (b)(3), (b)(5), and (b)(6).

23 18. On January 28, 2015, NSA sent a response letter to the plaintiff. In that letter, NSA
24 informed the plaintiff that it was withholding in full one (1) document that was responsive to the
25 request that had been referred to NSA by ODNI pursuant to FOIA exemptions (b)(1) and (b)(3).

26 ¹ NSA also had production deadlines under the order. The agency was required to
27 complete processing and produce any non-exempt, responsive material referred by ODNI by
28 February 2, 2015, to complete processing and produce non-exempt, responsive information from
responsive materials not requiring outside consultation by March 31, 2015, and to produce the
balance of its responsive materials by April 20, 2015.

1 19. On March 25, 2015, ODNI sent a final response letter to the plaintiff. In that letter
2 ODNI informed the plaintiff that it had located ten (10) documents containing information
3 responsive to its request. The letter further informed the plaintiff that it was releasing eight (8) of
4 those documents in segregable form with deletions made pursuant to FOIA exemption (b)(1), and
5 that the remaining two (2) were being withheld in full pursuant to exemptions (b)(1), (b)(3), and
6 (b)(5).

7 20. On March 31, 2015, NSA sent a response letter to the plaintiff. In that letter, NSA
8 informed the plaintiff that it had located documents that contained information that was responsive
9 to the request. The letter enclosed two (2) documents that NSA released in segregable form with
10 deletions made pursuant to FOIA exemptions (b)(1), (b)(3), (b)(5), and (b)(6); the letter also
11 indicated that two (2) additional responsive documents were being withheld in full pursuant to
12 FOIA exemptions (b)(1), (b)(3), and (b)(5).

13 21. On April 20, 2015, NSA sent a final response letter to the plaintiff. In that letter,
14 NSA informed the plaintiff that it had located additional documents containing information
15 responsive to its request. The letter informed the plaintiff that it was releasing three (3) of those
16 documents in segregable form with deletions made pursuant to FOIA exemptions (b)(1), (b)(3),
17 and (b)(5), and that the remaining ninety-one (91) documents were being withheld in full pursuant
18 to exemptions (b)(1), (b)(3), and (b)(5).

19 **III. EXPLANATION OF WITHHELD MATERIAL:**

20 **A. Exemption 1: classified information**

21 22. It is my understanding that Plaintiff is disputing only the redactions taken in one
22 document, Document 71, which was disclosed to Plaintiff on September 3, 2015. Document 71 is
23 entitled “Commercial and Government Information Technology and Industrial Control Product or
24 System Vulnerabilities Equities Policy and Process U//FOUO” (hereinafter “VEP Document”). It
25 was drafted and reviewed by an interagency working group and other stakeholders within the
26 United States Government and subsequently passed on to higher authority within the Executive
27 Branch as part of the Federal Government’s development of a vulnerabilities equities policy and
28 process. Vulnerabilities equities policy is the policy developed to define a process for Government

1 consideration of dissemination decisions regarding previously-unknown vulnerabilities discovered
2 within government information technology systems or other commercial information technology
3 or industrial control products or systems. Such vulnerabilities can significantly affect the
4 operation and safety of cryptographic and information systems used within national security
5 systems and US critical infrastructure.

6 23. The VEP Document was a document that the Government originally withheld in
7 full pursuant to exemptions (b)(1), (b)(3), and (b)(5). That denial was communicated to the
8 plaintiff in the ODNI's letter of January 15, 2015, and in the NSA's letter dated April 20, 2015.²

9 24. Subsequent to the issuance of the denial letters covering the VEP Document, the
10 Government re-processed the document to determine if any of the information contained within it
11 could be released. Because the VEP Document as drafted contains SECRET information, the
12 overall classification of the document was at the SECRET level.

13 25. As part of the re-processing of the VEP Document, the ODNI has identified that
14 certain information within the document continues to be classified and has withheld it under FOIA
15 exemption (b)(1) (5 U.S.C. § 552(b)(1)).

16 26. Exemption (b)(1) protects from release matters that are specifically authorized
17 under criteria established by an executive order to be kept classified in the interest of the national
18 defense or foreign policy, and are in fact properly classified pursuant to such executive order. 5
19 U.S.C. § 552(b)(1). The current executive order which establishes such criteria is Executive Order
20 13526 ("E.O. 13526").

21 27. Section 1.1 of E.O. 13526 provides that information may be originally classified if:
22 1) an original classification authority is classifying the information; 2) the information is owned
23 by, produced by or for, or is under the control of the Government; 3) the information falls within
24 one or more of the categories of information listed in section 1.4 of the Executive Order; and 4) the
25 original classification authority determines that the unauthorized disclosure of the information

26
27
28

² The VEP Document also appears in the holdings of the National Security Agency, also a party to this litigation.

1 reasonably could be expected to result in damage to the national security, and the original
2 classification authority is able to identify or describe the damage.

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

10 29. In addition, information shall not be considered for classification unless it falls
11 within one of the categories described in Section 1.4 of E.O. 13526. The relevant categories for
12 purposes of this case are § 1.4(c), which allows information to be classified if it pertains to
13 “intelligence activities (including covert action), intelligence sources or methods, or cryptology,”
14 and § 1.4(g), which protects “vulnerabilities or capabilities of systems, installations,
15 infrastructures, projects, plans, or protection services relating to the national security.”

16 30. I have personally and independently examined the portions of the document that
17 have been redacted under exemption (b)(1) as part of my responsibilities as an OCA at ODNI. As
18 a result of this examination, and after consulting with appropriate subject matter experts within the
19 ODNI and the relevant intelligence community agencies (including the NSA) which maintain
20 equities in the information, I have determined that the responsive information withheld under the
21 (b)(1) exemption remains currently and properly classified at the SECRET level, appropriately
22 withheld pursuant to E.O 13526, §§ 1.4(c) and 1.4(g), and exempt from disclosure pursuant to
23 FOIA exemption 1.

24 31. Generally, the redacted information contains details of the equities process that
25 would allow adversaries to exploit weaknesses in the Government’s computer systems by
26 identifying how the United States Government specifically handles such vulnerabilities when they
27 are identified. Its disclosure would enable adversaries to better target the VEP process and its
28 participants for counterintelligence and espionage purposes in order to obtain critical insights into

1 U.S. cyber operations and capabilities, or to take steps to circumvent U.S. Government measures to
2 protect Federal information systems. Vulnerability analysis has traditionally been performed by
3 individual departments and agencies, and the interagency sharing of the resulting information had
4 previously been performed on an ad-hoc basis. The VEP provides a routinized, repeatable and
5 internally transparent system for identifying, sharing information on, and closing cyber
6 vulnerabilities in order to minimize the possibility of harm to US citizens or interests. This unique
7 process of proactive sharing, if exposed, would likely be a target of interest for our adversaries
8 seeking to better understand and leverage the methodology for intelligence and counterintelligence
9 purposes.

10 32. Accordingly, information has been redacted in order to protect against that kind of
11 exploitation. We are withholding information that would provide insights into U.S. intelligence
12 cyber capabilities to collect on foreign adversaries. We are withholding information that contains
13 the U.S. Government's policies and processes employed in identifying and reporting cryptographic
14 vulnerabilities or vulnerabilities discovered in relation to a national security system and how and
15 when those vulnerabilities should be adjudicated and disseminated through the Vulnerabilities
16 Equities Process. We are also withholding information that relates to the specific considerations
17 (which have not been officially acknowledged) that the U.S. Government applies when a
18 vulnerability is identified. Finally, we are withholding information that would identify certain
19 agencies that participate in the process, the conditions under which each agency participates, the
20 timelines involved in the process, and the information that is submitted during the review process.

21 33. Disclosure of such above-described information reasonably could be expected to
22 cause serious damage to the national security because of the way that information, if revealed,
23 could be utilized by foreign intelligence services. Information on the government's cyber
24 capabilities and its cryptographic vulnerabilities would be of interest to foreign adversaries and,
25 once identified, would become a target of opportunity for collection by those services. It would be
26 useful for a foreign intelligence service to know what actions the government would take in
27 response to an identified vulnerability and the timing of those actions so that it could develop
28 countermeasures to ensure that it derives the greatest possible benefit from exploitation of that

1 vulnerability. A foreign intelligence service that has knowledge of all the government agencies
2 (both large and small) that participate in the VEP and the conditions under which they participate
3 has a roadmap for identifying potential targets of opportunity for recruitment and exploitation. If
4 unable to penetrate one agency, that service might look to penetrate a particular component of
5 another, smaller entity with the hope of obtaining more information about the VEP. Targeting U.S.
6 Government VEP participants would allow adversaries to gain unique insights into the
7 vulnerabilities discovered by U.S. Government elements—vulnerabilities which they could in turn
8 exploit to gain access to sensitive US Government networks—and would also allow such
9 adversaries to gain greater understanding of U.S. cyber operations and capabilities, which would
10 be used by those adversaries to further develop and improve their own capabilities to the detriment
11 of U.S. national security.

12 **B. Exemption 3: information protected by statute**

13 34. The ODNI and the NSA have also identified that information within the document
14 is properly withheld under FOIA exemption (b)(3), 5 U.S.C. § 552(b)(3).

15 35. Exemption 3 provides that FOIA does not require the production of records that are:
16 specifically exempted from disclosure by statute (other than section 552b of this
17 title), provided that such statute (A)(i) requires that the matters be withheld from
18 the public in such a manner as to leave no discretion on the issue, or (ii) establishes
19 particular criteria for withholding or refers to particular types of matters to be
20 withheld; and (B) if enacted after the date of enactment of the OPEN FOIA Act of
21 2009, specifically cites to this paragraph. 5 U.S.C. § 552(b)(3).³

22 36. Certain information contained in the VEP Document and withheld under (b)(3) falls
23 squarely within the scope of Section 102A(i)(1) of the National Security Act of 1947, as amended,
24 50 U.S.C. § 3024(i)(1). This statute provides that “the Director of National Intelligence shall
25 protect intelligence sources and methods from unauthorized disclosure.” The protection afforded
26 to intelligence sources and methods is absolute. Whether the sources and methods at issue are
27 classified is irrelevant for purposes of the protection afforded by 50 U.S.C. § 3024(i)(1).

28 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.

1 37. This statute recognizes the importance of protecting intelligence sources and
2 methods, including the methods and procedures utilized to identify vulnerabilities within
3 government communications systems and the role that the intelligence community plays in
4 addressing those vulnerabilities. The National Security Act entrusts the Director of National
5 Intelligence with responsibility for ensuring that protection.

6 38. As part of executing my responsibilities to the Director, I have reviewed the
7 contents of the VEP Document, including the information that has been withheld under exemption
8 (b)(3). I have also consulted with subject matter experts within the ODNI and with representatives
9 of the relevant agencies that maintain equities in the information, including the NSA. As a result
10 of that review, I have determined that intelligence sources and methods would be revealed if the
11 information redacted under exemption (b)(3) were to be released.

12 39. Specifically, certain withheld information implicates sources and methods such as
13 those employed to identify and address vulnerabilities within U.S. government information
14 systems and to protect research and development and critical infrastructure information necessary
15 to ensure the proper function of those information systems. This information requires protection
16 from unauthorized disclosure under the DNI's authority to protect intelligence sources and
17 methods under Section 102A(i) of the National Security Act of 1947, as amended [50 U.S.C. §
18 3024(i)].

19 40. Certain other information redacted in the VEP Document discusses the functions of
20 the NSA and its activities. I am invoking, on NSA's behalf and with its approval, Section 6 of the
21 National Security Agency Act of 1959, Pub. L. No. 86-36 [codified at 50 U.S.C. § 3605]. Section
22 6 provides that "[n]othing in this Act or any other law . . . shall be construed to require the
23 disclosure of the organization or any function of the National Security Agency, [or] of any
24 information with respect to the activities thereof. . . ." NSA's functions and activities are protected
25 from disclosure regardless of whether or not the information itself is classified. The information
26 withheld pursuant to Section 6 of the NSA Act pertains to NSA's role in adjudicating certain types
27 of vulnerabilities and certain of NSA's responsibilities as the Executive Secretariat for the VEP
28 process. As such, it relates directly to NSA functions and activities, including its responsibilities

1 as the “executive agent for the communications security of the United States Government” as
2 outlined in section 1.12(b)(8) of Executive Order 12333, and therefore falls within the scope of
3 the protection offered by Section 6 of the NSA Act.

4 **C. Exemption 5: deliberative process privilege**

5 41. Responsive information related to the deliberative process of creating the VEP has
6 been redacted from the header of each page of the document under exemption (b)(5). The
7 information contained in the redacted header reveals the recommendation forwarded by the
8 interagency working group involved in the creation of the VEP to a higher authority within the
9 Executive Branch, as well as a date reflecting the timing of that process.⁴ The redacted
10 information in the header also identifies the authority within the Executive Branch that would next
11 be reviewing this recommendation. Although this information does not identify the members of
12 that authority by name, it does provide a level of specificity that would tend to reveal particular
13 positions within the Government with minimal effort.

14 42. Disclosure of such information related to the deliberative process—what
15 recommendation was forwarded to whom, and the specific date on which a recommendation
16 moves to the next step in the deliberative process—could subject decision-makers to undue
17 pressure as they work to create an important process like the VEP. Exposing the recommendations
18 made at intermediate stages in the deliberative process to public scrutiny, regardless of whether
19 they were later accepted or rejected, could chill dialogue and lead to less open discussions while
20 the deliberative process is ongoing. Furthermore, interested onlookers could use such information
21 as they monitor future deliberative processes to scrutinize the progress of the deliberations,
22 pressuring decision-makers to accelerate their deliberations if they judged the process was not
23 progressing at the pace they desired. This, in turn, could damage the process, especially if it
24 involved the complex balancing of important goals such as national security and transparency, as
25 the VEP is designed to do.

26
27 ⁴ Although the redacted header does not expressly state the working group’s conclusions, it
28 conveys that the content within the document constitutes the recommendation of the group that is
being passed to the higher authority in the Executive Branch for review.

1 43. Additionally, to protect the integrity of the deliberative process that the VEP itself
2 undertakes each time it considers a particular vulnerability, certain specific groups identified as
3 participating in the VEP have been redacted under exemption (b)(5) in Sections 6.3, 6.6.1, 6.7,
4 6.7.1, 6.8, and Annex B of the VEP Document. The identity of the VEP participants that have
5 been withheld are those that have not been previously officially acknowledged, are frequent or
6 constant (rather than only occasional) participants in the process, and are typically relatively small
7 government components (as compared to entire Executive Departments). Public identification of
8 these participants in the VEP raises two risks.

9 44. First, given the public interest in the VEP, subjecting readily identifiable VEP
10 participants to public pressure could harm the integrity of the process itself, and undermine the
11 ability of the participants to appropriately consider the weighty issues they must address each time
12 they decide whether, when, or how a specific vulnerability should be disclosed.

13 45. Second, identifying this type of VEP participant increases the risk that they will be
14 the target of intelligence activities by foreign intelligence services. The VEP participants' work
15 implicates important equities because knowledge of undisclosed vulnerabilities can mean an
16 opportunity to collect crucial intelligence, potentially disrupt a terrorist attack, prevent the theft of
17 intellectual property, or even discover more dangerous vulnerabilities that are being used by
18 hackers or other adversaries to exploit our networks. In light of these stakes, there is a substantial
19 risk that these VEP participants will be targeted for espionage if their identities are known.
20 Disclosure of the identities of these VEP participants redacted under exemption (b)(5) would
21 therefore create counterintelligence risks similar to those discussed in paragraph 33 above.

22 **D. Segregability**

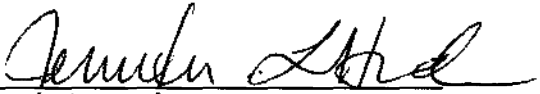
23 46. I reviewed the VEP Document for purposes of complying with FOIA's
24 segregability provision which requires the Government to release "any reasonably segregable
25 portion of a record" after proper application of the FOIA exemptions. 5 U.S.C. § 552(b). A line-
26 by-line review of the VEP Document was performed and all reasonably segregable, non-exempt
27 information has been released as evidenced, for example, by paragraphs 6.3, 6.6.1, 6.7.1, 6.8.2, and
28

1 7, which were previously portion marked as classified but have now been released in part and
2 redacted in part.

3 **CONCLUSION**

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

6 Executed this 30th day of October, 2015

7 

8 Jennifer L. Hudson
9 Director, Information Management Division
10 Office of the Director of National Intelligence
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28