Andrew Crocker (SBN 291596)
andrew@eff.org
Mark Rumold (SBN 279060)
mark@eff.org
Nathan Cardozo (SBN 259097)
nate@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy St.
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Attorneys for Plaintiff
Electronic Frontier Foundation

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

ELECTRONIC FRONTIER FOUNDATION, Plaintiff, v. NATIONAL SECURITY AGENCY, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, Defendants.	Case No.: 14-cv-03010-RS **NOTICE OF MOTION AND CROSS MOTION FOR SUMMARY JUDGMENT AND OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT** Date: February 18, 2016 Time: 1:30 pm Courtroom 3—17th Floor Hon. Richard Seeborg

NOTICE OF MOTION

PLEASE TAKE NOTICE that on February 18, at 1:30 pm in the United States Courthouse at San Francisco, California, Plaintiff, Electronic Frontier Foundation ("EFF"), will, and hereby does, cross move this Court for summary judgment on all of its claims.

Pursuant to Federal Rule of Civil Procedure 56, EFF seeks a court order requiring the government to release records under the Freedom of Information Act, 5 U.S.C. § 552. EFF respectfully asks that this Court issue an order requiring the government to release all records improperly withheld from the public. This cross motion is based on this notice of motion, the memorandum of points and authorities in support of this cross motion, the Declaration of Andrew Crocker ("Crocker Decl.") and attached exhibits in support of this cross motion, and all papers and records on file with the Clerk or which may be submitted prior to or at the time of the hearing, and any further evidence which may be offered.

DATED: December 4, 2015

Respectfully submitted,

/s/ Andrew Crocker

Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
Attorneys for Plaintiff
ELECTRONIC FRONTIER FOUNDATION

TABLE OF CONTENTS

NOTICE OF MOTION i

MEMORANDUM OF POINTS AND AUTHORITIES 1

INTRODUCTION 1

BACKGROUND 2

PROCEDURAL HISTORY OF THIS CASE 5

ARGUMENT 5

I. FOIA Establishes a Presumption of Disclosure, and the Government Bears the Burden of Demonstrating That Withheld Information Is Clearly Exempt. 6

II. The Government's Reliance on Exemptions 1 and 3 Is Unlawful Because It Has Already Disclosed Information It Is Now Withholding. 8

A. The Government Has Officially Acknowledged That It Uses Vulnerabilities for Offensive Purposes. 9

B. The Government Has Officially Acknowledged the Specific Policy Considerations Involved in the VEP. 12

C. These Official Disclosures Preclude Withholding of Information Concerning Offensive Capabilities and Policy Considerations from the VEP Document. 14

III. Exemption 5 Does Not Support Withholding the Timing of the VEP Document or the Participants Named in the Document. 15

A. The VEP Document Has Been Adopted. 16

B. The Deliberative Process Privilege Does Not Apply to the Specific Information Defendants Have Withheld Because It Is Not Deliberative. 18

1. The deliberative process privilege does not apply to the header information in the VEP Document. 19

2. The deliberative process privilege does not apply to the "names of small government components" in the VEP Document. 20

IV. The Court Should Conduct an *In Camera* Review of the VEP Document and Order Defendants to Release All Improperly Withheld Information. 22

CONCLUSION 24

TABLE OF AUTHORITIES

Federal Cases

ACLU v. CIA,
710 F.3d 422 (D.C. Cir. 2013) 15

Afshar v. Dep't of State,
702 F.2d 1125 (D.C. Cir. 1983) 14

AIDS Healthcare Foundation v. Leavitt,
256 F. App'x 954 (9th Cir. 2007) 21

Alfred A. Knopf, Inc. v. Colby,
509 F.2d 1362 (4th Cir. 1975) 14

Allen v. CIA,
636 F.2d 1287 (D.C. Cir. 1980) 23, 24

Arthur Andersen v. IRS,
679 F.2d 254 (D.C. Cir. 1982) 16

Bay Area Lawyers Alliance for Nuclear Arms Control v. Dep't of State,
818 F. Supp. 1291 (N.D. Cal. 1992) 19

Birch v. USPS,
803 F.2d 1206 (D.C. Cir. 1986) 7

Brennan Ctr. for Justice v. Dep't of Justice,
697 F.3d 184 (2d Cir. 2012) 16, 18

Brinton v. Dep't of State,
636 F.2d 600 (D.C. Cir. 1980) 21

Celotex Corp. v. Catrett,
477 U.S. 317 (1986) 7

Coastal States Gas Corp. v. Dep't of Energy,
617 F.2d 854 (D.C. Cir. 1980) 16, 18, 19, 22

Dep't of Air Force v. Rose,
425 U.S. 352 (1976) 15

Dep't of Interior v. Klamath Water Users Protective Ass'n,
532 U.S. 1 (2001) 6

Dep't of Justice v. Reporters Comm. for Freedom of the Press,
489 U.S. 749 (1989) 6, 7

Dep't of Justice v. Tax Analysts,
492 U.S. 136 (1989) 6

EPA v. Mink,
410 U.S. 73 (1973) 19

Feshbach v. SEC,
5 F. Supp. 2d 774 (N.D. Cal. 1997) 7

Fitzgibbon v. CIA,
911 F.2d 755 (D.C. Cir. 1990) 5, 8, 9, 14

Goldberg v. Dep't of State,
818 F.2d 71 (D.C. Cir. 1987) 7

Jones v. FBI,
41 F.3d 238 (6th Cir. 1994) 24

Judicial Watch, Inc. v. Dep't of Treasury,
796 F. Supp. 2d 13 (D.D.C. 2011) 20

King v. Dep't of Justice,
830 F.2d 210 (D.C. Cir. 1987) 7

Mead Data Cent., Inc. v. Dep't of Air Force,
566 F.2d 242 (D.C. Cir. 1977) 7

N.Y. Times Co. v. Dep't of Justice,
756 F.3d 100 (2d. Cir. 2014) 14, 15

Nat'l Council of La Raza v. Dep't of Justice,
411 F.3d 350 (2d Cir. 2005) 18

Nat'l Wildlife Fed'n v. U.S. Forest Serv.,
861 F.2d 1114 (9th Cir. 1988) 6

NLRB v. Robbins Tire & Rubber Co.,
437 U.S. 214 (1978) 5, 6

NLRB v. Sears, Roebuck & Co.,
421 U.S. 132 (1975) 6, 16, 19, 20

Pub. Citizen, Inc. v. OMB,
598 F.3d 865 (D.C. Cir. 2009) 18

Quarles v. Dep't of Navy,
893 F.2d 390 (D.C. Cir. 1990) 19

Spirko v. USPS,
147 F.3d 992 (D.C. Cir. 1998) 22

Students Against Genocide v. Dep't of State,
257 F.3d 828 (D.C. Cir. 2001) 15

Tax Reform Research Grp. v. IRS,
419 F. Supp. 415 (D.D.C. 1976) 21

Taxation With Representation Fund v. IRS,
646 F.2d 666 (D.C. Cir. 1981) 18

Vaughn v. Rosen,
484 F.2d 820 (D.C. Cir. 1973) 7

Wolfe v. Dep't of Health & Human Servs.,
839 F.2d 768 (D.C. Cir. 1988) 19, 20

Federal Statutes

5 U.S.C. § 552(a) 7, 16, 22

5 U.S.C. § 552(b) 6, 23

Federal Rules

Fed. R. Civ. P. 56(a) 7

Directives

Dep't of Defense, *DOD Directive O-3600.01 "Information Operations"* (Aug. 14, 2006) 11

Other Authorities

Andy Greenberg, *Meet the Hackers Who Sell Spies the Tools to Crack Your PC (and Get Paid Six-Figure Fees)*, Forbes (Mar. 21, 2012) 2

David E. Sanger, *Obama Lets NSA Exploit Some Internet Flaws, Officials Say*, N.Y. Times (Apr. 12, 2014) 2, 9

David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. Times (June 1, 2012) 3

Ellen Nakashima & Joby Warrick, *Stuxnet Was Work of U.S. and Israeli Experts, Officials Say*, Wash. Post (June 2, 2012) 3

Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, Wired (July 11, 2011) 3

Michael Riley, *NSA Said to Exploit Heartbleed Bug for Intelligence for Years*, Bloomberg (Apr. 11, 2014) 4

Nicole Perlroth & David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, N.Y. Times (July 13, 2013) 2

NSA, *Discovering IT Problems, Developing Solutions, Sharing Expertise* (Oct. 30, 2015) 11

President's Review Grp. on Intel. & Commc'ns. Techs., *Liberty and Security in a Changing World* (Dec. 12, 2013) 3, 4

MEMORANDUM OF POINTS AND AUTHORITIES

INTRODUCTION

Over the past two years, the American public, industry, press, and the government have been engaged in expansive public discussion of the government's intelligence gathering techniques and policies. Part of that public debate has focused on the government's knowledge and use of "zero days," software flaws or vulnerabilities.[1] Zero days can be put to "offensive" use by an attacker exploiting knowledge of the flaw to gain access to computer systems, compromise security, intercept sensitive information, or otherwise compromise weaknesses in software. On the other hand, the "defensive" use of vulnerabilities involves disclosing them to software vendors or other responsible entities and enabling them to be "patched" against such attacks.

The subject of this lawsuit under the Freedom of Information Act is a single document, the government's written policy called the Vulnerabilities Equities Process ("VEP"), which describes how the government weighs the trade-offs between these offensive and defensive uses of vulnerabilities. Because the government's decisions about whether to disclose vulnerabilities to the vendor or hold them for future exploitation can have far-reaching consequences for both information security and user privacy, Plaintiff the Electronic Frontier Foundation ("EFF") sought to obtain the VEP from Defendants ODNI and NSA. Despite extensive public description of the content of the VEP by government officials, Defendants claimed that not a single word of the document could be released pursuant to FOIA. Subsequently, Defendants changed course and released the VEP Document with redactions. However, the document still contains unjustified redactions. These redactions are not supported by the law, and the Court should order the VEP produced for *in camera* inspection. That inspection will reveal that the government's withholdings are unjustified in light of the substantial public disclosure concerning the VEP's content, so the Court should deny the

[1] They are so named because the software developer has no time and hence "zero days" to resolve or patch the flaw.

Defendants' motion for summary judgment and grant Plaintiff's cross-motion.

BACKGROUND

Software Vulnerabilities and the Government's Use of Zero Days

According to the government, federal agencies routinely acquire knowledge of "previously-unknown vulnerabilities discovered within government information technology systems or other commercial information technology or industrial control products or systems." Declaration of Jennifer L. Hudson ¶ 22 ("Hudson Decl."), ECF No. 32-3. This includes vulnerabilities in "commercial and open source software" that is used by hundreds of millions of people—operating systems such as Windows and Apple OS X, web browsers such as Chrome and Firefox, word processing applications such as Microsoft Word, plug-ins such as Adobe Flash, and basic security protocols—running on individual laptops, smartphones, and tablets. Crocker Decl. Ex. A (ODNI, *Statement on Bloomberg News story that NSA knew about the "Heartbleed bug" flaw and regularly used it to gather critical intelligence* (Apr. 11, 2014) ("ODNI Blog Post")).[2] The government learns of these vulnerabilities through its own research and by purchasing information about them from third parties who specialize in finding exploitable bugs.[3] Once the government knows about vulnerabilities, it can then use them to access targeted devices or users for a variety of purposes, including surveillance and "cyberattacks."[4] In one high-profile instance, the U.S. government and Israel used several zero days as part of a "cyberweapon" known as "Stuxnet," which targeted industrial control

[2] *See also* David E. Sanger, *Obama Lets NSA Exploit Some Internet Flaws, Officials Say*, N.Y. Times (Apr. 12, 2014), http://www.nytimes.com/2014/04/13/us/politics/obama-lets-nsa-exploit-some-internet-flaws-officials-say.html.

[3] *See, e.g.*, Nicole Perlroth & David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, N.Y. Times (July 13, 2013), http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html; Andy Greenberg, *Meet the Hackers Who Sell Spies the Tools to Crack Your PC (and Get Paid Six-Figure Fees)*, Forbes (Mar. 21, 2012), http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees.

[4] Sanger, *Obama Lets NSA Exploit Some Internet Flaws, Officials Say*, *supra*.

systems running at Iranian nuclear enrichment plants and successfully destroyed hundreds of centrifuges by causing them to spin too fast.[5]

The Presidential Review Group's Recommendations on Zero Days

In August 2013, following the intense public debate sparked by news reports and official acknowledgment of a range of government surveillance programs, President Obama appointed an expert Review Group on Intelligence and Communications Technologies. The Review Group produced a final report in December 2013, with forty-six recommendations "designed to protect our national security and advance our foreign policy while also respecting our longstanding commitment to privacy and civil liberties[.]"[6] On zero days, the Review Group concluded that "in almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection."[7] As a result, it recommended that the government clarify its policy with regard to disclosure of zero days:

> "We recommend that the National Security Council staff should manage an interagency process to review on a regular basis the activities of the US Government regarding attacks that exploit a previously unknown vulnerability in a computer application or system. . . . US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks. In rare instances, US policy may briefly authorize using a Zero Day for high priority intelligence collection, following senior, interagency

[5] David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. Times (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html; Ellen Nakashima & Joby Warrick, *Stuxnet Was Work of U.S. and Israeli Experts, Officials Say*, Wash. Post (June 2, 2012), https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html; Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, Wired (July 11, 2011), http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet.

[6] President's Review Grp. on Intel. & Commc'ns. Techs., *Liberty and Security in a Changing World* at 1 (Dec. 12, 2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[7] *Id.* at 220.

review involving all appropriate departments."[8]

The Vulnerabilities Equities Process

In April 2014, the government made a series of public disclosures about its knowledge and use of vulnerabilities in response to a Bloomberg News report that the NSA had exploited a serious flaw in a protocol used to keep a very large percentage of the world's websites secure.[9] The story prompted an immediate response by the ODNI. Crocker Decl. Ex. A (ODNI Blog Post). Although it denied the accusation that the government had exploited the specific vulnerability in the Bloomberg story, the ODNI explained that "[w]hen Federal agencies discover a new vulnerability . . . it is in the national interest to responsibly disclose the vulnerability rather than to hold it for an investigative or intelligence purpose . . . [u]nless there is a clear national security or law enforcement need[.]" *Id.* It further explained that in response to recommendations by the White House Review Group discussed above, the executive branch had "reviewed its policies in this area and reinvigorated an interagency process for deciding when to share vulnerabilities. This process is called the Vulnerabilities Equities Process." *Id.*

In a follow-up post on the official White House blog later that month, Special Assistant to the President and Cybersecurity Coordinator Michael Daniel described the VEP as "principles to guide agency decision-making" and explained that it was an "existing policy with respect to disclosing vulnerabilities" that was being reinvigorated "so that everyone can have confidence in the integrity of the process we use to make these decisions." Crocker Decl. Ex. B, at 1-2 (Michael Daniel, White House, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities* (Apr. 28, 2014) ("White House Blog Post")). Daniel acknowledged that the government may sometimes "withhold[] knowledge of some vulnerabilities for a limited time," because doing so might present "an opportunity to collect crucial intelligence that could

[8] *Id.* at 37.

[9] Michael Riley, *NSA Said to Exploit Heartbleed Bug for Intelligence for Years*, Bloomberg (Apr. 11, 2014), http://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html.

thwart a terrorist attack[,] stop the theft of our nation's intelligence property, or even discover more dangerous vulnerabilities." He also listed the specific considerations involved when the government withholds knowledge of a vulnerability for these purposes. *Id*. at 2-3.

PROCEDURAL HISTORY OF THIS CASE

Plaintiff substantially agrees with Defendants' summary of the procedural history of this case as detailed in their memorandum and the Hudson Declaration. Defs.' Mem. at 2-3; Hudson Decl. ¶¶ 10-25. However, Plaintiff notes that Defendants initially withheld the VEP document in full pursuant to Exemptions 1, 3 and 5. Hudson Decl. ¶ 23. The parties agreed to narrow the scope of this lawsuit to this single document and file cross summary judgment motions, with the Defendants to file first, on August 12, 2015. ECF No. 24. Just prior to the date Defendants were scheduled to file their motion, they determined that the VEP Document, previously withheld in full, could be reprocessed. ECF No. 27 (filed Aug. 11, 2015). Defendants then released a 13-page document, the majority of which was non-exempt. *See* Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process U//FOUO ("VEP Document"), ECF No. 32-4.

ARGUMENT

FOIA safeguards the public's ability to hold the government accountable. *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978). Here, using the press and its own public relations outlets, the government has made statements that reveal much of the information in the VEP it has subsequently withheld in this lawsuit. As such, this "official acknowledgement" overcomes whatever otherwise valid exemption the government might assert. *See Fitzgibbon v. CIA,* 911 F.2d 755, 765 (D.C. Cir. 1990).

In addition, the VEP represents the government's final agency policy concerning zero days. Accordingly, the deliberative process privilege does not allow for withholding

information like that contained within the VEP Document, which the government has formally adopted. *See NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 152 (1975). Under any circumstances, the deliberative process privilege does not apply to the specific information withheld from the VEP Document.

For the reasons that follow, the Court should order the VEP produced for *in camera* inspection, EFF's cross-motion for summary judgment should be granted, and the government's motion for summary judgment should be denied.

I. FOIA Establishes a Presumption of Disclosure, and the Government Bears the Burden of Demonstrating That Withheld Information Is Clearly Exempt.

FOIA safeguards the American public's right to know "what their Government is up to." *Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 773 (1989). The central purpose of the statute is "to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed." *Robbins*, 437 U.S. at 242.

FOIA requires disclosure of all agency records at the request of the public unless the records fall within one of nine narrow exemptions. *See* 5 U.S.C. § 552(b). These "limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act." *Dep't of Interior v. Klamath Water Users Protective Ass'n*, 532 U.S. 1, 8 (2001) (citation omitted). The exemptions "have been consistently given a narrow compass," and agency records that "do not fall within one of the exemptions are improperly withheld." *Dep't of Justice v. Tax Analysts*, 492 U.S. 136, 151 (1989) (internal quotation marks omitted). Even where exemptions apply, FOIA explicitly requires that "[a]ny reasonably segregable potion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt[.]" 5 U.S.C. § 552(b).

FOIA disputes involving the propriety of agency withholdings are commonly resolved on summary judgment. *See, e.g.*, *Nat'l Wildlife Fed'n v. U.S. Forest Serv.*, 861 F.2d 1114, 1115 (9th Cir. 1988). Summary judgment is proper when the moving party shows that "there is

no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a); *Feshbach v. SEC*, 5 F. Supp. 2d 774, 779 (N.D. Cal. 1997) (citing *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986)). In FOIA cases, a court reviews the government's decision to withhold records *de novo*, and the government bears the burden of proving records have been properly withheld. 5 U.S.C. § 552(a)(4)(B); *Reporters Comm.*, 489 U.S. at 755. Even national security claims of the type invoked here do not alter a court's "independent responsibility" to undertake a thorough *de novo* evaluation of the government's withholdings. *Goldberg v. Dep't of State*, 818 F.2d 71, 76-77 (D.C. Cir. 1987) (noting Congress amended FOIA to clarify its "intent that courts act as an independent check on challenged classification decisions").

To satisfy its burden to withhold information, the agency "must provide a relatively detailed justification [for its withholding decisions], specifically identifying the reasons why a particular exemption is relevant and correlating those claims with the particular part of a withheld document to which they apply." *Mead Data Cent., Inc. v. Dep't of Air Force*, 566 F.2d 242, 251 (D.C. Cir. 1977) (citations omitted).[10] "Unlike the review of other agency action that must be upheld if supported by substantial evidence and not arbitrary or capricious, the FOIA expressly places the burden 'on the agency to sustain its action.'" *Reporters Comm.*, 489 U.S. at 755 (quoting 5 U.S.C. § 552(a)(4)(B)). Thus, when claiming one of FOIA's exemptions, the agency bears the burden of demonstrating to a reviewing court that withheld information is "*clearly* exempt." *Birch v. USPS,* 803 F.2d 1206, 1209 (D.C. Cir. 1986) (emphasis added) (citing *Vaughn*, 484 F.2d at 823).

[10] In *Vaughn v. Rosen,* 484 F.2d 820 (D.C. Cir. 1973), the D.C. Circuit established the procedural requirements that "an agency seeking to avoid disclosure" must follow in order to carry its burden in a FOIA case. *Id*. at 828. These procedural obligations are typically satisfied by the submission of an index describing each withheld record (a "*Vaughn* index") and an affidavit from an agency official, further describing the agency's rationale for withholding the record. *See King v. Dep't of Justice*, 830 F.2d 210, 219 (D.C. Cir. 1987). The government has submitted both here. *See* Hudson Decl., ECF No. 32-3 and Draft *Vaughn* Index, ECF No. 32-5.

II. The Government's Reliance on Exemptions 1 and 3 Is Unlawful Because It Has Already Disclosed Information It Is Now Withholding.

Although the government asserts FOIA Exemptions 1 and 3 to withhold portions of the VEP Document, the withheld information has already been publicly disclosed by the government in other circumstances. Such official and public disclosures work to overcome even an otherwise valid FOIA exemption. *Fitzgibbon,* 911 F.2d at 765 ("When information has been 'officially acknowledged,' its disclosure may be compelled even over an agency's otherwise valid exemption claim."). Accordingly, neither Exemptions 1 nor 3 authorize the government's withholdings.

The government has explained that the purpose of the VEP is to weigh so-called equities—competing interests within the government such as disclosing and fixing vulnerabilities on one hand, and withholding and exploiting them on the other. Because the government cannot meet both interests at the same time, the VEP establishes a mediating procedure that allows it to reach a "dissemination decision" to disclose or withhold a vulnerability. VEP Document at 1.

However, in the redacted VEP Document provided to Plaintiff, the government has illegally withheld at least two categories of information. First, it has released only information pertaining to decisions to disclose vulnerabilities and correspondingly redacted all references to decisions to retain and exploit vulnerabilities for so-called offensive purposes, despite clear-cut admissions at all levels of government that "offensive" uses are contemplated by the VEP. Second, it has withheld information about the actual policy considerations involved in weighing these equities in order to reach a decision—again, despite having already disclosed those considerations in other contexts.

These official and public disclosures, taken together, constitute an "official acknowledgement" of the government's offensive use of zero days and the policy considerations undertaken through the VEP. For purposes of FOIA, an official acknowledgment must meet three criteria:

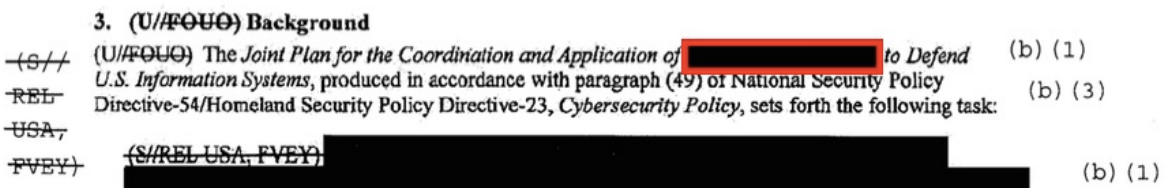
> First, the information requested must be as specific as the information previously released. Second, the information requested must match the information previously disclosed[.] . . . Third, . . . the information requested must already have been made public through an official and documented disclosure.

Fitzgibbon, 911 F.2d at 765. The government's statements about the withheld information meets these criteria.

A. The Government Has Officially Acknowledged That It Uses Vulnerabilities for Offensive Purposes.

The government's retention and use of vulnerabilities for offensive purposes has not only long been a matter of public record,[11] it has also been confirmed by government officials in documented public statements and by publicly released government documents.

In at least one instance, publicly released documents appear to match *verbatim* information withheld from the VEP Document. Section 3 of the VEP Document, "Background," states: "The *Joint Plan for the Coordination and Application of [redacted] to Defend U.S. Information Systems*, produced in accordance with paragraph 49 of National Security Policy Directive-54/Homeland Security Policy Directive-23, *Cybersecurity Policy*, sets forth the following task[.]" VEP Document at 1.


3. (U//~~FOUO~~) Background

~~(S//REL USA, FVEY)~~ (U//~~FOUO~~) The *Joint Plan for the Coordination and Application of* [redacted] *to Defend U.S. Information Systems*, produced in accordance with paragraph (49) of National Security Policy Directive-54/Homeland Security Policy Directive-23, *Cybersecurity Policy*, sets forth the following task:

~~(S//REL USA, FVEY)~~ [redacted] (b) (1) (b) (3) (b) (1)

Redacted text in the VEP Document.

However, Paragraph 49 of National Security Policy Directive-54 has been publicly disclosed, and it is echoed in a document released to Plaintiff in this very FOIA. Crocker Decl. Ex. C (White House, *National Security Presidential Directive/NSPD54, Homeland Security Presidential Directive/HSPD-23* (Jan. 8, 2008)); Ex. D (Vulnerabilities Equities Process Highlights). The redacted words are "offensive capabilities":

[11] *See* Sanger, *Obama Lets NSA Exploit Some Internet Flaws, Officials Say*, *supra.*

(49) Within 120 days of the date of this directive, the Secretaries of State, Defense, and Homeland Security, the Attorney General, and the DNI shall submit to the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism a joint plan for the coordination and application of offensive capabilities to defend U.S. information systems. (U//~~FOUO~~)

Unredacted text in publicly released version of NSPD-54. See Crocker Decl. Ex. C, at 3.

This is far from the only official acknowledgement that the government exploits vulnerabilities for offensive purposes. The April 2014 blog post by White House Cybersecurity Coordinator Michael Daniel and a follow-up interview with Mr. Daniel in *Wired* magazine also confirm the government's offensive use of vulnerabilities. For example, Daniel wrote that pursuant to the VEP, the government may "withhold[] knowledge of some vulnerabilities for a limited time," because doing so presents "an opportunity to collect crucial intelligence that could thwart a terrorist attack[,] stop the theft of our nation's intelligence property, or even discover more dangerous vulnerabilities[.]" Crocker Decl. Ex. B, at 2 (White House Blog Post). Similarly, he told *Wired* that there "are a limited set of vulnerabilities that we may need to retain for a limited period of time in order to conduct legitimate national security intelligence and law enforcement missions." Crocker Decl. Ex. E, at 7 (Kim Zetter, *U.S. Gov Insists It Doesn't Stockpile Zero-Day Exploits To Hack Enemies* (Nov. 17, 2014) (Interview with White House Cybersecurity Coordinator Michael Daniel) ("Michael Daniel Wired Interview")). In the same vein, in a May 2014 interview, newly retired NSA Director General Keith Alexander echoed the trade-off between offensive and defensive uses of software vulnerabilities:

> NSA has to understand and identify all the vulnerabilities—the coding errors, backdoors, zero days etc—in the technology tools that our governments relies on to safeguard those systems from exploitation by adversaries. . . . To ask NSA not to look for weaknesses in the technology that we use, and to not seek to break the codes our adversaries employ to encrypt their messages is, I think, misguided. I would love to have all the terrorists just use that one little sandbox over there so that we could focus on them. But they don't.

Crocker Decl. Ex. F, at 3.

Additional examples abound in documents released to Plaintiff as part of its FOIA. For example, a document disclosed to Plaintiff by Defendant ODNI consists of notes from the working group that wrote the VEP Document and includes the discussion question of "What information does the Offense need[] from the Defense." Crocker Decl. G, at 2 (*NSPD-54/HSPD-23 Paragraph (49) Plan Working Group CNCI Connect the Centers Team Meeting Agenda* (July 28, 2008)). Another document disclosed by ODNI includes a description of some equities considered by the working group:

> This is even more important for cybersecurity activities, which can take many forms: defense (CND), *offense (CNA),* investigation (CNI), as well as counterintelligence (CI). These activities are all linked and properly coordinated can enable each other and close gaps an enemy might otherwise exploit. Proper coordination should begin with a firm understanding of the 'equities' involved and agreements on where equities lie for cybersecurity activities and stakeholders.

Crocker Decl. H (emphasis added).[12]

And an NSA blog post published the same day as Defendants filed their motion for summary judgment quantifies the percentage of vulnerabilities the NSA discloses compared to those it exploits: "Historically, NSA has released more than 91% of vulnerabilities discovered in products that have gone through our internal review process and that are made or used in the United States. The remaining 9% were either fixed by vendors before we notified them, or not disclosed for national security reasons. . . . Disclosing a vulnerability means we forgo an opportunity to collect crucial foreign intelligence that could thwart a terrorist attack[.]"[13]

Even without access to the exact wording of other redactions in the VEP Document, it is clear that the government has unlawfully withheld multiple references to and discussion of

---

[12] According to a Defense Department Directive released pursuant to FOIA, CNA stands for "Computer Network Attack" which is defined as an "[o]peration[] to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." Dep't of Defense, *DOD Directive O-3600.01 "Information Operations"* (Aug. 14, 2006) at 9, *available at* https://fas.org/irp/doddir/dod/info_ops.pdf.

[13] NSA, *Discovering IT Problems, Developing Solutions, Sharing Expertise* (Oct. 30, 2015), https://www.nsa.gov/public_info/news_information/2015/ncsam/discovering_solving_sharing_it_solutions.shtml

"offensive capabilities." For example, "Annex A – Equities" begins with a large block of text redacted pursuant to Exemptions 1 and 3. Immediately following this redaction is a paragraph with the heading "Defensive Cyber Operations Community Equities." It is clear to even a casual reader that previous paragraph discusses offensive equities. Similarly, in Section 6.8, "Decision Implementation," subsection 6.8.1 "Decision Implementation: Restrict Dissemination" is completed redacted, while subsection 6.8.2 "Decision Implementation: Disseminate" is almost entirely unredacted. Given the government's public acknowledgment that it weighs equities between "defensive" disclosure and "offensive" retention, it is highly likely that the redacted information pertains to offensive uses. Other unsupportable redaction of the government's offensive use of zero days almost certainly exists throughout the document, supporting the need for the Court to conduct an *in camera* inspection of the unredacted VEP.

B. The Government Has Officially Acknowledged the Specific Policy Considerations Involved in the VEP.

Government officials have also acknowledged the *specific* policy considerations that participants in the VEP employ when determining whether to disclose a vulnerability. In the blog post on the White House's website, Cybersecurity Coordinator Michael Daniel listed a series of considerations involved when the government withholds knowledge of a vulnerability for intelligence purposes:

> How much is the vulnerable system used in the core internet infrastructure, in other critical infrastructure systems, in the U.S. economy, and/or in national security systems?
> Does the vulnerability, if left unpatched, impose significant risk?
> How much harm could an adversary nation or criminal group do with knowledge of this vulnerability?
> How likely is it that we would know *if someone else was exploiting it*?
> *How badly do we need the intelligence we think we can get from exploiting the vulnerability?*
> Are there other ways we can get it?
> Could we *utilize the vulnerability* for a short period of time before we disclose it?

> How likely is it that someone else will discover the vulnerability?
> Can the vulnerability be patched or otherwise mitigated?

Crocker Decl. Ex. B, at 2-3 (White House Blog Post).

Additionally, in a speech at Stanford University, NSA Director Admiral Mike Rogers listed strikingly similar policy considerations involved in vulnerabilities disclosure decisions:

> [T]he greatest numbers of vulnerabilities we find, we share. . . . [But t]here are some instances in which we are not going to do that. And the thought process, as we go through this from a policy side as we make this deliberate decision—the kinds of things we tend to look at are, how foundational and widespread is this potential vulnerability? Who tends to use it? Is it something that, you know, you'll generally find in one particular nation-state or a particular segment, or is this pretty wide across a large swathe for the U.S. and for others? How likely do we think others are able to likely find it? Is this the only way to potentially—for us to generate the insights? Is there another alternative here that we could use?

Crocker Decl. Ex. I, at 7.

In addition to further confirming the offensive exploitation of vulnerabilities to gain "intelligence" on other "nation-states," these policy considerations clearly reflect a common set of criteria used in the VEP, including:

1. How widely used and foundational the vulnerability is, including in U.S. government systems, critical infrastructure and other systems crucial to national stability;
2. Whether adversaries to the U.S. could cause harm to these systems if the vulnerability is not disclosed;
3. The magnitude and/or significance of the risk posed by the vulnerability;
4. Whether the vulnerability is suited to offensive use;
5. How likely it is that others will find the vulnerability;
6. What alternatives to exploiting the vulnerability exist; and
7. Whether the vulnerability can be easily patched.

Despite this official acknowledgement, the government has redacted policy considerations, most obviously in VEP Document Section 6.2 "Process Considerations," and likely elsewhere throughout the document, such as Sections 6.8.1 and 6.8.2, further supporting the need for *in camera* review.

C. These Official Disclosures Preclude Withholding of Information Concerning Offensive Capabilities and Policy Considerations from the VEP Document.

Taken together, these disclosures satisfy the standard for "official acknowledgement" of both categories of information withheld by the government pursuant to Exemptions 1 and 3. *See Fitzgibbon,* 911 F.2d at 765. First, the disclosed information "match[es]" the withheld information. *Id.* As demonstrated above, at least one of the government's redactions matches an already public document *exactly*. In other instances, the official disclosures match the redactions in the VEP Document identically even if the wording of the withheld information is not verbatim because the test does not "require absolute identity." *N.Y. Times Co. v. Dep't of Justice*, 756 F.3d 100, 120 (2d. Cir. 2014). This is because a "FOIA requester would have little need for undisclosed information if it had to match precisely information previously disclosed."[14] *Id.* Second, the information is "as specific" as that withheld. *Fitzgibbon*, 911 F.2d at 765. The public disclosures by government officials pertain directly to the VEP and the government's use of vulnerabilities for offensive purposes as well as its specific policy considerations, just as the redactions do. Third, the information was made public through both "official and documented disclosure[s]." *Id*. The disclosures were "official": Michael Daniel (as White House Cybersecurity Coordinator) and Admiral Mike Rogers and General Keith Alexander (as the current and former heads of the NSA respectively) are all government officials directly involved in the VEP. *See Afshar v. Dep't of State*, 702 F.2d 1125, 1130 (D.C. Cir. 1983) (noting public disclosure by "an authoritative source" constitutes official acknowledgement); *see also Alfred A. Knopf, Inc. v. Colby,* 509 F.2d 1362, 1370 (4th Cir. 1975) ("It is one thing for a reporter or author to speculate or guess that a thing may be so or even, quoting undisclosed sources, to say that it is so; it is quite another thing for one in a position to know of it officially to say that it is so."). The disclosures are also "documented:"

[14] The Second Circuit also noted that *Fitzgibbon* derives the three-part test for official acknowledgement from *Afshar v. Dep't of State*, 702 F.2d 1125, 1133 (D.C. Cir. 1983), which "does not mention a requirement that the information sought match the information previously disclosed." *N.Y. Times*, 756 F.3d at 120 n.19 (internal quotations omitted).

Daniel's blog post is on the White House website, and the interviews with Daniel, Rogers, and Alexander are readily available on the Internet. *See* Crocker Decl. Exs. A, B, E, F, I; *see also Students Against Genocide v. Dep't of State*, 257 F.3d 828, 836 (D.C. Cir. 2001) ("For the public domain doctrine to apply, the specific information sought must have already been disclosed and preserved in a permanent public record.") (internal citations and quotations omitted).

"With the redactions and public disclosures discussed above, it is no longer either 'logical' or plausible' to maintain that disclosure" of the VEP Document "risks disclosing any aspect of . . . intelligence activities, [or] sources and methods." *See N.Y. Times*, 756 F.3d at 120. Although the government may wish to deny or ignore these official disclosures, FOIA was intended pry from "possibly unwilling official hands" government information "shielded unnecessarily" from the public. *Dep't of Air Force v. Rose,* 425 U.S. 352, 361 (1976) (internal quotation marks omitted). As the D.C. Circuit has noted, "[t]here comes a point where . . . Court[s] should not be ignorant as judges of what [they] know as men and women. We are at that point with respect" to the redacted information in the VEP Document. *ACLU v. CIA*, 710 F.3d 422, 431 (D.C. Cir. 2013) (internal citations omitted).

III. Exemption 5 Does Not Support Withholding the Timing of the VEP Document or the Participants Named in the Document.

Defendants have claimed FOIA Exemption 5's deliberative process privilege to withhold two categories of information from the VEP Document: (1) Header information relating to the "timing" of the "process" of the "working group involved in the creation of VEP" and the working group's "recommendation;" and (2) names of "certain specific groups identified as participating in the VEP . . . in Sections 6.3, 6.6.1, 6.7, 6.7.1, 6.8, and Annex B of the VEP Document." Hudson Decl. ¶¶ 41-43.

Defendants' reliance upon the deliberative process privilege fails for two reasons: First, Defendants have adopted the VEP Document as the government's "effective law and policy" on the issue. Second, regardless of this adoption, the deliberative process privilege does not

apply to the narrowly defined types of information the Defendants have withheld from the VEP Document.

A. The VEP Document Has Been Adopted.

Because FOIA expressly requires that agencies make available "final opinions" and "statements of policy and interpretations which have been adopted by the agency," *see* 5 U.S.C. §§ 552(a)(2)(A), (B), the Supreme Court has explained that such documents may never be withheld under Exemption 5. *Sears*, 421 U.S. at 154. As a corollary, in *Sears* the Court also determined that otherwise privileged documents can lose any protection they might previously have held when "an agency chooses expressly to adopt or incorporate by reference" the document as the agency's final decision or determination. 421 U.S. at 161; *see also Brennan Ctr. for Justice v. Dep't of Justice*, 697 F.3d 184, 196-197 (2d Cir. 2012) (describing adoption as the alternate "path" to a disputed record's loss of Exemption 5's protections). Thus, even if a document—or a portion thereof—may come within the deliberative process privilege at the time it is prepared, it can "lose that status if it is adopted, formally or informally, as the agency position on an issue." *Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 866 (D.C. Cir. 1980); *see also Arthur Andersen v. IRS*, 679 F.2d 254, 257-58 (D.C. Cir. 1982) (same). Adoption requires only that a record be "expressly" adopted within the agency, not that the adoption be public, formal, or repeated. *Sears*, 421 U.S. at 161.

Here, there is ample evidence that the VEP Document has been formally adopted by the government.

First, as described above, the parties mutually agreed to narrow the scope of the issues remaining to the single document representing "the *final* interagency Vulnerabilities Equities Process . . . as described in the April 2014 White House blog post by Michael Daniel." ECF No. 24, at 5 (emphasis added). The VEP Document—the single document at issue here—is that final document.

Second, statements by government officials confirm that the government uses the VEP Document as its policy when deciding whether to disclose vulnerabilities. In the White House blog post referenced in the parties' stipulation, Cybersecurity Coordinator Michael Daniel wrote that in response to the Bloomberg News story, the White House "re-invigorated our efforts to implement *existing* policy with respect to disclosing vulnerabilities." Crocker Decl. Ex. B, at 1-2 (White House Blog Post) (emphasis added). Similarly, Defendant ODNI wrote that the White House had "*reviewed its policies* in this area and reinvigorated an interagency process . . . called the Vulnerabilities Equities Process." Crocker Decl. Ex. A (ODNI Blog Post.) (emphasis added). When questioned by *Wired* as to why the existing policy needed to be "reinvigorated," Michael Daniel explained that the VEP was established in 2010 but was "not implemented to the full degree that it should have been," and thus those involved needed to "make sure it was actually happening consistently and as thoroughly as the policy called for." Crocker Decl. Ex. E, at 4-5 (Michael Daniel Wired Interview). Hence, these statements confirm the VEP Document was formally adopted as policy in 2010 by the government, although the government's subsequent adherence to this policy may have been lacking.

Third, other documents released by Defendants pursuant to FOIA also confirm that the VEP Document is the sole representation of the government's policy for handling vulnerability disclosure. For example, the VEP "Highlights" document disclosed by Defendant ODNI explains that the "end result of the [Vulnerabilities Equities Process] working group is a community-wide coordinated document," the VEP Document. Crocker Decl. Ex. D. Similarly, a 2014 FBI presentation entitled "Use of Zero Days & Policy" explains that recipients of the presentation should have received an email with the VEP Document, which is a "policy document . . . dated 2/16/10."[15] Crocker Decl. Ex. J, at 7 (FBI, *Use of Zero Days & Policy* (Apr. 24, 2014)).

[15] Given this official public statement revealing the date on the VEP document, the redacted timing information from the header has also been officially acknowledged and cannot be withheld for this reason as well. *See* Section II, *supra*.

Such agency action—approving, public references in non-privileged agency documents and in statements to the public—demonstrates agency adoption of the VEP document. *See, e.g.*, *Taxation With Representation Fund v. IRS*, 646 F.2d 666, 678 (D.C. Cir. 1981) (noting that deliberative process privilege may evaporate if a document "is used by the agency in its dealings with the public") (quoting *Coastal States*, 617 F.2d at 866); *Brennan Center*, 697 F.3d at 204 (holding a footnote reference in a public document and congressional testimony "taken together establish express adoption"); *Nat'l Council of La Raza v. Dep't of Justice*, 411 F.3d 350, 357 (2d Cir. 2005) ("references to the OLC Memorandum made by the Attorney General and his high-ranking advisors, the substance of their comments, and the way in which their comments were used—that is, to assure third parties as to the legality of the actions the third parties were being urged to take"—demonstrated adoption) (internal footnote omitted).

B. The Deliberative Process Privilege Does Not Apply to the Specific Information Defendants Have Withheld Because It Is Not Deliberative.

Because Defendants have formally adopted the VEP Document, the deliberative process privilege does not apply. But, even setting adoption aside, the deliberative process privilege still does not protect the two types of withheld material in the VEP Document—header information and the names of small government components participating in the VEP. This material is not "deliberative" within the meaning of the privilege.

Documents are "deliberative only if they reflect[ ] advisory opinions, recommendations, and deliberations comprising part of a process by which governmental decisions and policies are formulated, [or if they reflect] the personal opinions of the writer prior to the agency's adoption of a policy." *Pub. Citizen, Inc. v. OMB*, 598 F.3d 865, 875 (D.C. Cir. 2009) (internal quotations omitted). This is because the purpose of the privilege is to "assure that subordinates within an agency will feel free to provide the decisionmaker with their uninhibited opinions and recommendations without fear of later being subject to public ridicule or criticism . . . [and] protect against premature disclosure of proposed policies before they have been finally formulated or adopted." *Coastal States*, 617 F.2d at 866.

Because the deliberative process privilege is intended to increase candor by protecting deliberative material, it does not extend to "factual information," unless disclosure of this information "would reflect or reveal the deliberative process" itself.[16] *Bay Area Lawyers Alliance for Nuclear Arms Control v. Dep't of State*, 818 F. Supp. 1291, 1297 (N.D. Cal. 1992) (citing *Coastal States*, 617 F.2d at 866-67); *see also EPA v. Mink*, 410 U.S. 73, 93 (1973).

The material the Defendants have withheld here is factual. Moreover, because the VEP Document is "final," there is no deliberative process for this information to reveal. *Sears*, 421 U.S. at 161. Thus, the deliberative process privilege does not apply, and the cases cited by Defendants in support of their withholdings are inapposite.

1. The deliberative process privilege does not apply to the header information in the VEP Document.

The header information in VEP Document, which consists of dates and information that "conveys that the content within the document constitutes [a] recommendation" to a higher authority, Hudson Decl. ¶ 42 n.4, is factual and not covered by the privilege. The government's suggestion that disclosure of this information, although factual, would "so expose the deliberative process that it must be covered by the [deliberative process] privilege" is unavailing. Defs.' Mem. at 13 (quoting *Wolfe v. Dep't of Health & Human Servs.*, 839 F.2d 768, 774 (D.C. Cir. 1988)).

Contrary to Defendants' arguments, the circumstances in *Wolfe* are not analogous. There, the D.C. Circuit considered proposed rules forwarded between several agencies and held that they were "unquestionably predecisional" for the very reason that they were still proposed rules in the process of being considered by the participating agencies. 839 F.2d at 774. Thus, the dates that the proposed rules were forwarded were properly withheld as deliberative because they would "disclose that proposals had been made" and the

[16] Indeed, while the rationale behind the deliberative process privilege encourages candor in deliberative discussions, the requirement that facts must be disclosed enhances the integrity of agency deliberations. *See Quarles v. Dep't of Navy*, 893 F.2d 390, 392 (D.C. Cir. 1990) (noting that "the prospect of disclosure is less likely to make an advisor omit or fudge raw facts").

"recommended outcome . . . at each stage," which "would certainly reveal policies prematurely." *Id.* at 774-75. Here, by contrast, Defendants have stated unequivocally that the VEP Document represents the final interagency policy on vulnerability equities and that this process was completed and adopted in 2010. *See* Section III.A, *supra*. Hence there is no risk of "chill[ing] discussion at a time when agency opinions are fluid and tentative," *id.* at 776, or of putting time pressure on officials, since the decision to adopt the VEP Document already occurred in the past.[17] *Sears*, 421 U.S. at 151-52. This is true even for the header information that "conveys" that the VEP Document constitutes the recommendation of its authors, since this recommendation was likely to adopt the document, which the government subsequently did. *Id.*

Additionally, Defendants make no attempt to explain how *Wolfe* supports withholding the information that the government claims "would tend to reveal particular positions within the Government with minimal effort," such as the "authority within the Executive Branch" receiving the VEP Document. Hudson Decl. ¶ 41; Defs.' Mem. at 16. Because the VEP Document is "final," there is no opportunity for members of the public to identify this authority and put undue pressure on it prior to a final decision. More fundamental, because the document is final, there is no good reason for the public to be prevented from knowing which authority within the government approved it. *Sears*, 421 U.S. at 152.

2. The deliberative process privilege does not apply to the "names of small government components" in the VEP Document.

The deliberative process privilege similarly does not extend to the names of "small government components" participating in the VEP from Sections 6.3, 6.6.1, 6.6, 6.7 and Annex B in the VEP Document.

[17] For the same reasons, *Judicial Watch, Inc. v. Dep't of Treasury*, 796 F. Supp. 2d 13 (D.D.C. 2011) is inapposite. There, the plaintiff did not dispute that the deliberative process privilege applied to an internal Treasury Department memo, so the court relied on *Wolfe* to uphold withholding of timing information about this deliberative process. *Id.* at 28.

In arguing that this information is privileged, Defendants elide the distinction between the long-finished process of finalizing the VEP Document and future hypothetical deliberative processes surrounding the adjudication of specific vulnerabilities. As is clear from the document itself, the VEP Document merely sets forth the steps that the government will follow and the considerations involved in adjudicating specific vulnerabilities. Defendants have not asserted that the VEP document contains information about the participants in any specific "dissemination decision." Indeed, in asserting that the names of small government components are privileged, Ms. Hudson says only that "onlookers could monitor *future* deliberative processes" and exert pressure on participants "*each time* they decide whether, when, or how a *specific* vulnerability should be disclosed." Hudson Decl. ¶¶ 42, 44 (emphasis added).

Thus, the cases cited by Defendants do not support withholding this information. In *AIDS Healthcare Foundation v. Leavitt*, 256 F. App'x 954, 957 (9th Cir. 2007), for example, the Ninth Circuit upheld the extremely narrow withholding of the names of individual decision-makers for *specific* grant applications filed by the plaintiff, not the names of decision-makers participating in the grant review process generally—which were already publicly known. Here, by contrast, the Defendants have withheld the names of agency components from the *general* procedure described in the VEP Document, not from "the deliberative process that the VEP itself undertakes each time it considers a *particular* vulnerability." Hudson Decl. ¶ 43 (emphasis added). Other cases cited by the Defendants involve deliberative process privilege protections for authors of deliberative documents and participants in an ongoing deliberative process. *Brinton v. Dep't of State*, 636 F.2d 600, 604-05 (D.C. Cir. 1980); *Tax Reform Research Grp. v. IRS*, 419 F. Supp. 415, 423 (D.D.C. 1976). But the names of "small government components" listed in the VEP Document fall into neither of these categories; instead they are simply named in a document that has been adopted and does not itself qualify for the deliberative process privilege.

Finally, Defendants' claim that identifying these "small government components" "increases the risk that they will be the target of intelligence activities by foreign intelligence

services," Hudson Decl. ¶ 45, is both unsupported and not an appropriate use of Exemption 5. As described above, the purpose of Exemption 5 is to protect the integrity of the agency's decision-making process by facilitating candor and preventing against premature disclosure of inchoate proposals. *Coastal States*, 617 F.2d at 866. To the extent that the Defendants are concerned about the risk of the government components becoming the target of foreign espionage, that is not an interest protected by the deliberative process privilege.[18] *Id*.

IV. The Court Should Conduct an *In Camera* Review of the VEP Document and Order Defendants to Release All Improperly Withheld Information.

Defendants' declarations submitted in support of their summary judgment filings cannot govern the resolution of this case: the Court's *in camera* review of the unredacted VEP Document is necessary. FOIA empowers the Court in conducting *de novo* review to examine "agency records *in camera* to determine whether such records or any part thereof shall be withheld." 5 U.S.C. § 552(a)(4)(B). Given the circumstances present here and brevity of the single document at issue, *in camera* review would quickly and effectively resolve this case.

"A judge has discretion to order *in camera* inspection on the basis of an uneasiness, on a doubt" before taking "responsibility for a de novo determination." *Spirko v. USPS*, 147 F.3d 992, 996 (D.C. Cir. 1998) (internal quotations omitted). In light of Defendants' failure to fulfill their duties under the FOIA**,** Plaintiff respectfully submits that the Court has ample reason here for "uneasiness" and "doubt" regarding Defendants' positions that there is no additional information that can be released from the VEP document.

Defendants state that they have "disclosed all non-exempt information that reasonably could be disclosed." Defs' Mem. at 18; Hudson Decl. ¶ 46. That claim is not credible. Defendants previously withheld the *entire* VEP Document on the grounds that they could not

[18] Indeed, despite invoking this risk under the deliberative process privilege, Defendants candidly admit that their concerns are "similar to those discussed" in the section of their brief dealing with Exemption 1 and cite to a paragraph of the Hudson Declaration that describes Ms. Hudson's reasons for withholding entirely separate information under Exemption 1. *See* Defs.' Mem. at 18 (citing Hudson Decl. ¶ 33).

reasonably segregate *any* non-exempt information, only to determine on the eve of this summary judgment proceeding that the majority of the document could in fact be segregated and released. ECF No. 24 at 5. Now, as demonstrated above, Defendants continue to withhold as exempt information that has been officially acknowledged by government officials. This includes information that has been disclosed *verbatim* pursuant to this very request. *See* Section II.A *supra* (redaction of the words "offensive capabilities" from Section 3 of the VEP Document). Tellingly, the classification markings accompanying that redaction indicate that the text withheld was originally *unclassified* and was only marked classified and withheld prior to the document's production. This suggests that Defendants' classification determinations (and corresponding redactions) are inconsistent at best.

Defendants' Exemption 5 withholdings are also demonstrably arbitrary. Defendants state that during the course of preparing their motion, they "determined" that the names of two government agencies in the VEP Document previously withheld as deliberative—the Secret Service and the NSA—could be disclosed. Defs.' Mem. at 3; *compare* ECF No. 32-4 at 5 *with* ECF No. 32-6 at 5. Nowhere do they explain why these agencies, and not others, are no longer protected by the deliberative process privilege.

Moreover, although Ms. Hudson states that "[a] line-by-line review of the VEP Document was performed and all reasonably segregable, non-exempt information has been released," Hudson Decl. ¶ 46, the examples discussed above underscore the need for this Court's searching review of the Defendants' compliance with FOIA's obligation to provide "[a]ny reasonably segregable potion" of the records at issue in this case. *See* 5 U.S.C. § 552(b).

Finally, there is a "greater call for *in camera* inspection" in "cases that involve a strong public interest in disclosure." *Allen v. CIA*, 636 F.2d 1287, 1298 (D.C. Cir. 1980). As the D.C. Circuit has explained, (in language particularly pertinent here):

> When citizens request information to ascertain whether a particular agency is properly serving its public function, the agency often deems it in its best interest to stifle or inhibit the probes. It is in these instances that the judiciary plays an important role in reviewing the agency's withholding of information.

> But since it is in these instances that the representations of the agency are most likely to be protective and perhaps less than accurate, the need for *in camera* inspection is greater.

Id. at 1299; *see also Jones v. FBI*, 41 F.3d 238, 243 (6th Cir. 1994) (noting *in camera* inspection warranted where there is "*strong public interest*—where the effect of disclosure or exemption clearly extends to the public at large") (emphasis in original). The document at issue in this case is the topic of intense public scrutiny into whether Defendants are properly serving their public functions, a fact acknowledged by Defendant ODNI when it granted expedited processing for Plaintiff's initial request. Compl. ¶ 18. And as the recommendations of the President's Review Group, as well as Cybersecurity Coordinator Michael Daniel's statements indicate, the substance of the government's vulnerability disclosure policy affects millions of individuals. In light of this overriding public interest, the need for *in camera* inspection is particularly acute.[19]

CONCLUSION

For the foregoing reasons, the government's motion for summary judgment should be denied, and EFF's Cross Motion for summary judgment should be granted.

Respectfully submitted,

DATED: December 4, 2015

/s/ Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
Andrew Crocker, Esq.
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
Attorney for Plaintiff

[19] Indeed, this is precisely the approach taken by another member of this Court in a case involving documents disclosed after similarly overbroad representations about classification and segregability and a strong public interest in the withheld documents. *See* Order Re: Production of Docs. for In Camera Review at 2-3, *EFF v. Dep't of Justice*, No. 11-5221 (N.D. Cal. June 13, 2014), ECF No. 85.