

ORAL ARGUMENT NOT YET SCHEDULED

No. 13-5369

IN THE UNITED STATES COURT OF APPEALS
DISTRICT OF COLUMBIA CIRCUIT

ELECTRONIC PRIVACY INFORMATION CENTER

Plaintiff-Appellant,

v.

NATIONAL SECURITY AGENCY

Defendant-Appellee.

On Appeal from the
United States District Court
for the District of Columbia

JOINT APPENDIX

MARC ROTENBERG

Counsel of Record

ALAN BUTLER

GINGER MCCALL

JULIA HORWITZ

DAVID HUSBAND

Electronic Privacy Information Center

1718 Connecticut Ave. NW

Suite 200

Washington, DC 20009

(202) 483-1140

Counsel for Plaintiff-Appellant

Electronic Privacy Information Center

TABLE OF CONTENTS

Electronic Privacy Information Center v. National Security Agency
(Docket No. 13-5369)

<u>Case No.</u>	<u>Document Title</u>	<u>Page(s)</u>
10-196	Memorandum Opinion by Judge Beryl A. Howell Granting in Part and Denying in Part Defendant's Motion for Summary Judgment	JA 000001
10-196	Civil Docket Report Through 03/11/2014	JA 000026
10-196	Complaint for Injunctive Relief Filed by Plaintiff EPIC	JA 000031
10-196	Answer to Complaint for Injunctive Relief Filed by Defendant NSA	JA 000042
10-196	Memorandum Opinion by Judge Beryl A. Howell Granting Defendant's Partial Motion to Dismiss	JA 000051
10-196	Defendant's Motion for Summary Judgment	JA 000067
	Attachments:	
	Declaration of Diane M. Janosek	JA 000093
	Declaration of Mary Ronan	JA 000109
	Tab A (EPIC FOIA Request)	JA 000116
	Tab B (NSA FOIA Response)	JA 000122
	Tab C (EPIC FOIA Appeal)	JA 000125
	Tab D (NSA Letter Granting Expedited Processing)	JA 000140
	Tab E (NSA Response Letter – August 14, 2009)	JA 000142
	Tab F (NSA Response Letter – October 26, 2009)	JA 000146
	Tab G (EPIC Second FOIA Appeal)	JA 000149
	Defendant's Statement of Material Facts Not in Dispute	JA 000182
10-196	Plaintiff's Cross Motion for Summary Judgment	---
	Attachments:	
	Plaintiff's Statement of Material Facts Not in Dispute	JA 000188
	Plaintiff's Statement of Genuine Issues in	JA 000192

<u>Case No.</u>	<u>Document Title</u>	<u>Page(s)</u>
	Opposition to Defendant's SMF	
10-196	Defendant's Memorandum in Opposition to Plaintiff's Cross Motion for Summary Judgment	---
	Attachments:	
	Defendant's Statement of Genuine Issues in Opposition to Plaintiff's SMF	JA 000194
10-196	Minute Order of September 9, 2013	JA 000196
10-196	Joint Status Report – September 16, 2013	JA 000197

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY
INFORMATION CENTER,

Plaintiff,

v.

NATIONAL SECURITY AGENCY,

Defendant.

Civil Action No. 10-196 (BAH)

Judge Beryl A. Howell

MEMORANDUM OPINION

The plaintiff, Electronic Privacy Information Center (“the plaintiff” or “EPIC”), brings this action under the Freedom of Information Act, 5 U.S.C. § 552, claiming that the defendant, the National Security Agency (“the defendant” or “NSA”), wrongfully withheld responsive records to a FOIA request seeking the unredacted text of National Security Presidential Directive (“NSPD”) 54 and related documents.¹ Compl. ¶¶ 15, 55, ECF No. 1. Pending before the Court are the defendant’s Motion for Summary Judgment, ECF No. 12, and the plaintiff’s Cross-Motion for Summary Judgment, ECF No. 13. For the reasons set forth below, both motions are granted in part and denied in part.

I. BACKGROUND

A. Factual History

1. *National Security Presidential Directive 54*

The main document at issue here, NSPD 54, also known as Homeland Security Presidential Directive 23 (“HSPD 23”), was issued by then-President George W. Bush on

¹ Although not fully described in the Complaint, these related documents, as made clear in the parties’ briefing, are IAD Management Directive 20 and NSA/CSS 1-58.

January 8, 2009. Declaration of Diane M. Janosek, Deputy Associate Director for Policy and Records, NSA, (“Janosek Decl.”) ¶ 8, ECF No. 12-2. “NSPD 54 is a confidential communication from the President of the United States to a select and limited group of senior foreign policy advisors, cabinet officials, and agency heads on the subject of cybersecurity policy.” Decl. of Mary Ronan, Director of Access Management Office, National Security Staff (“Ronan Decl.”) ¶ 7, ECF No. 12-10; *see also* Def.’s Mem. Supp. Mot. for Summ. J. (“Def.’s Mem.”) at 3, ECF No. 12-1. “NSPD 54 also implemented the [Comprehensive National Cybersecurity Initiative (“CNCI”).” Janosek Decl. ¶ 8. It was distributed with a “transmittal memo” from the Homeland Security Council’s Executive Secretary that “emphasized NSPD-54’s close-hold nature and the need to safeguard its content.” Ronan Decl. ¶ 7. This transmittal memo “prohibited dissemination of the document beyond its authorized recipients without White House approval and further instructed that even within receiving agencies, copies should be distributed only on a need to know basis.” *Id.* The document is classified “Top Secret” but includes portions that are unclassified.² *Id.* ¶ 8.

2. *The Plaintiff’s FOIA Request*

In June 2009, the plaintiff submitted a FOIA request to the NSA seeking “National Security Presidential Directive 54 . . . and related records” from the defendant. Janosek Decl. Tab A at 3, ECF No. 12-3. Specifically, the FOIA request sought: (1) “The text of the National Security Presidential Directive 54 otherwise referred to as The Homeland Security Presidential

² There is some dispute as to how much of, and at what level, NSPD 54 is classified. The defendant asserts it is withholding all of NSPD under Exemption 5 as a “presidential communication,” but it also asserts that one paragraph is being withheld under Exemption 1 “because the information is currently and properly classified in accordance with [Executive Order] 13526 and Exemption 3 because the information is protected by statutes.” Janosek Decl. ¶ 34. The NSC’s declarant, however, states “NSPD-54 as a whole is classified as TOP SECRET. Individual paragraphs within NSPD-54 have different classification markings ranging from UNCLASSIFIED to, SECRET, and TOP SECRET.” Ronan Decl. ¶ 8. It is unnecessary to determine at what level, if any, NSPD 54 is classified because, as explained in part III.A *infra*, NSPD 54 is not an “agency record” for the purposes of the FOIA under the D.C. Circuit’s recent opinion in *Judicial Watch v. United States Secret Service*, 726 F.3d 208 (D.C. Cir. 2013).

Directive 23[;]” (2) “The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation[;]” and (3) “Any privacy policies related to either the Directive, [or] the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative.” *Id.* at 5.³ On August 14, 2009, the defendant released two redacted documents, USSID SP0018 and NSA/CSS Policy 1-23, responsive to the third part of the plaintiff’s request that had been previously released pursuant to the FOIA.⁴ Janosek Decl. ¶ 13. With that release, the defendant notified the plaintiff that other responsive records had also been located and were under review “to determine what information could be released and the [the defendant] would finish [its] review as expeditiously as possible.” *Id.*

By letter dated October 26, 2009, the defendant informed the plaintiff that it had no records responsive to the second part of the plaintiff’s request. Janosek Decl. Tab F at 1, ECF No. 12-8. Of the three documents responsive to the first and third parts of the plaintiff’s request, two were being withheld in their entirety under FOIA Exemption 5, 5 U.S.C. § 552(b)(5), which exempts from disclosure “inter-agency or intra-agency memoranda or letters which would not be available by law to a party in litigation with the agency.” Janosek Decl. Tab F at 1. Portions of the same documents were also being withheld under FOIA Exemption 1, 5 U.S.C. § 552(b)(1), which exempts from disclosure items properly classified. *Id.* at 1–2. The third document was not released as it “did not originate with this Agency” and had “been referred to the National Security Council for review and direct response to [the plaintiff].” *Id.* at 2.

³ The request also sought expedited processing and a request for a fee waiver. Janosek Decl. Tab A at 5–6. The fee waiver was granted but expedited processing was initially denied. Janosek Decl. ¶ 11. After an administrative appeal, the request for expedited processing was granted. *Id.* ¶ 12.

⁴ The defendant does not specify to whom the documents had been previously released. *See* Janosek Decl. ¶ 13; Janosek Decl. Tab E at 2, ECF No. 12-7.

The plaintiff timely filed an administrative appeal of these determinations. Janosek Decl. ¶ 17. While the appeal was pending, the plaintiff timely filed the instant action. *Id.* The defendant subsequently released redacted copies of IAD Management Directive 20 and NSA/CSS 1-58, which were the two documents it referred to in the October 26, 2009 letter as being withheld in their entirety under Exemption 5. *Id.* ¶ 15 n.2. Portions of those documents continued to be withheld under Exemptions 1 and 3. *Id.* Thus, at issue in this case are the portions of IAD Management Directive 20 and NSA/CSS 1-58 withheld under Exemptions 1 and 3, and NSPD 54. *Id.* NSPD 54 is the document that did not originate with the defendant agency, and is being withheld in its entirety under the presidential communications privilege portion of Exemption 5, 5 U.S.C. § 552(b)(5), with one paragraph also being withheld under Exemptions 1 and 3. *See* Janosek Decl. ¶ 34.

B. Procedural History

The plaintiff filed the instant action against the Defendant and the National Security Council (“NSC”) asserting four claims for relief regarding the defendant’s alleged failure to comply with the FOIA’s statutory deadlines and to disclose responsive agency records (Counts One and Two); the National Security Council’s alleged failure to disclose responsive agency records (Count 3); and the defendant’s alleged violation of the Administrative Procedure Act, 5 U.S.C. § 706 (Count 4). *See* Compl. ¶¶ 52–73. The Complaint seeks production of all responsive records, a *Vaughn* index describing all records withheld and the exemptions under which they are being withheld, and attorneys’ fees. *Id.* at 10–11.

The defendant and the NSC filed a partial motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim as to Counts Three and Four and to dismiss all claims against the NSC. *See* Def.’s Partial Mot. to Dismiss at 1, ECF No. 4. This motion was granted because the NSC is not an “agency” within the meaning of the FOIA, *see* Mem. Op. at

8–9, ECF No. 9, and adequate relief is available to the plaintiff under the FOIA without resort to the APA. *See id.* at 14.

Now pending before the Court are the parties’ cross motions for summary judgment on the remaining counts, Counts One and Two. After the motions were fully briefed, the D.C. Circuit released its opinion in *Judicial Watch, Inc. v. United States Secret Service*, 726 F.3d 208 (D.C. Cir. 2013) (“*Judicial Watch*”), which, for the first time, applied the “control” test for whether a record is an “agency record” set forth in *United We Stand America, Inc. v. IRS*, 359 F.3d 595 (D.C. Cir. 2004) (“*United We Stand*”), to the Office of the President. *See Judicial Watch*, 726 F.3d at 231. The Court invited the parties to supplement their briefing as to whether NSPD 54 was an “agency record” under the *United We Stand* test. *See* Minute Order dated September 9, 2013. The parties declined to do so. *See* Joint Status Report at 1, ECF No. 26. The motions are now ripe for decision.

II. LEGAL STANDARD

Congress enacted the FOIA as a means “to open agency action to the light of public scrutiny.” *Am. Civil Liberties Union v. U.S. Dep’t of Justice*, 655 F.3d 1, 5 (D.C. Cir. 2011) (quoting *Dep’t of Air Force v. Rose*, 425 U.S. 352, 361 (1976)). The Supreme Court has “consistently recognized [] the basic objective of the Act is disclosure.” *Chrysler Corp. v. Brown*, 441 U.S. 281, 290 (1979). At the same time, the statute represents a “balance [of] the public’s interest in governmental transparency against legitimate governmental and private interests that could be harmed by release of certain types of information.” *United Techs. Corp. v. U.S. Dep’t of Def.*, 601 F.3d 557, 559 (D.C. Cir. 2010) (internal citations omitted). Reflecting that balance, the FOIA contains nine exemptions set forth in 5 U.S.C. § 552(b), which “are explicitly made exclusive and must be narrowly construed.” *Milner v. U.S. Dep’t of Navy*, 131

S. Ct. 1259, 1262 (2011) (internal quotations and citations omitted) (citing *FBI v. Abramson*, 456 U.S. 615, 630 (1982)); see also *Pub. Citizen, Inc. v. Ofc. of Mgmt. and Budget*, 598 F.3d 865, 869 (D.C. Cir. 2010). “[T]hese limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act.” *Rose*, 425 U.S. at 361.

The agency invoking an exemption to the FOIA has the burden “to establish that the requested information is exempt.” *Fed. Open Mkt. Comm. of the Fed. Reserve Sys. v. Merrill*, 443 U.S. 340, 351-352 (1979); see also *Assassination Archives & Research Ctr. v. CIA*, 334 F.3d 55, 57 (D.C. Cir. 2003) (holding that the agency “bears the burden of establishing the applicability of the claimed exemption.”). In order to carry this burden, an agency must submit sufficiently detailed affidavits or declarations, a *Vaughn* index of the withheld documents, see *Vaughn v. Rosen*, 484 F.2d 820, 827 (D.C. Cir. 1973), or both, to demonstrate that the government has analyzed carefully any material withheld, to enable the court to fulfill its duty of ruling on the applicability of the exemption, and to enable the adversary system to operate by giving the requester as much information as possible, on the basis of which he can present his case to the trial court. *Oglesby v. U. S. Dep’t of Army*, 79 F.3d 1172, 1176 (D.C. Cir. 1996) (“The description and explanation the agency offers should reveal as much detail as possible as to the nature of the document, without actually disclosing information that deserves protection...[which] serves the purpose of providing the requestor with a realistic opportunity to challenge the agency’s decision.”).

A district court must review the *Vaughn* index and any supporting declarations “to verify the validity of each claimed exemption.” *Summers v. Dep’t of Justice*, 140 F.3d 1077, 1080 (D.C. Cir. 1998). The FOIA provides federal courts with the power to “enjoin the agency from withholding records and to order the production of any agency records improperly withheld from

the complainant.” 5 U.S.C. 552(a)(4)(B).

Summary judgment is appropriate when “there is no genuine dispute as to any material fact.” FED. R. CIV. P. 56. “In FOIA cases, ‘[s]ummary judgment may be granted on the basis of agency affidavits if they contain reasonable specificity of detail rather than merely conclusory statements, and if they are not called into question by contradictory evidence in the record or by evidence of agency bad faith.’” *Judicial Watch*, 726 F.3d at 215 (D.C. Cir. 2013) (quoting *Consumer Fed’n of Am. v. U.S. Dep’t of Agric.*, 455 F.3d 283, 287 (D.C. Cir. 2006) and *Gallant v. NLRB*, 26 F.3d 168, 171 (D.C. Cir. 1994)). “Ultimately, an agency’s justification for invoking a FOIA exemption is sufficient if it appears ‘logical’ or ‘plausible.’” *Judicial Watch, Inc. v. U.S. Dep’t of Defense*, 715 F.3d 937, 941 (D.C. Cir. 2013) (quoting *ACLU v. U.S. Dep’t of Defense*, 628 F.3d 612, 619 (D.C. Cir. 2011)); *Larson v. U.S. Dep’t of State*, 565 F.3d 857, 862 (D.C. Cir. 2009) (quoting *Wolf v. CIA*, 473 F.3d 370, 374-75 (D.C. Cir. 2007)).

III. DISCUSSION

The parties have focused their attention on whether the withholding of records responsive to the plaintiff’s request under exemptions to the FOIA was proper, but such exemptions are irrelevant if the records requested are not “agency records” within the meaning of the FOIA. *See Judicial Watch*, 726 F.3d at 214–15. If the records in question are not “agency records,” courts do not have the power under the FOIA to order their disclosure.⁵ *See id.*; *see also* 5 U.S.C.

⁵ Whether a document is an “agency record” is a jurisdictional question that must be answered before proceeding to decide a case under the FOIA on the merits. *See Kissinger v. Reporters Comm. for Freedom of the Press*, 445 U.S. 136, 150 (1980) (“Under 5 U.S.C. § 552(a)(4)(B), federal jurisdiction is dependent upon a showing that an agency has (1) ‘improperly’; (2) ‘withheld’; (3) ‘agency records.’ Judicial authority to devise remedies and enjoin agencies can only be invoked, under the jurisdictional grant conferred by § 552.”); *Judicial Watch, Inc. v. Fed. Hous. Fin. Agency*, 646 F.3d 924, 926 (D.C. Cir. 2011) (“[U]nder FOIA, a federal court may only order an agency to release ‘agency records.’”); *Glick v. Dep’t of Army*, 971 F.2d 766, *1 (D.C. Cir. 1992) (per curiam) (affirming dismissal of FOIA suit because “[a]ppellant does not allege that any agency records have been improperly withheld, which is a jurisdictional prerequisite to suit under the FOIA.”). The courts have “an independent obligation to determine whether subject-matter jurisdiction exists.” *Citizens for Responsibility and Ethics in Wash. v. U.S. Dep’t of Homeland Sec.*, 532 F.3d 860, 862 (D.C. Cir. 2008) (citing *Nat’l Mining Ass’n v. Kempthorne*, 512 F.3d 702, 706

§ 552(a)(4)(B). Thus, the Court will first determine if the primary document at issue, NSPD 54, is an “agency record” before turning to a discussion of the propriety of any exemptions. Next, it will review the application of Exemptions 1 and 3 to IAD Management Directive 20 and NSA/CSS 1-58. Finally, the Court will turn to the plaintiff’s challenge to the defendant’s interpretation of the second portion of the plaintiff’s request.

A. NSPD 54 Is Not An Agency Record

The defendant withheld NSPD 54 under Exemption 5 and, consequently, the majority of the parties’ briefing centers on whether this exemption’s incorporation of the “presidential communications privilege” applies to NSPD 54.⁶ See, Pl.’s Mem. Opp’n to Def.’s Mot. Summ. J. and in Supp. Pl.’s Cross-Mot. for Summ. J. (“Pl.’s Mem.”) at 10–21, ECF No. 14; Def.’s Mem. at 7–12. In doing so, the parties gloss over the question of whether NSPD 54 is an “agency record” at all, which is a threshold question the Court must resolve before turning to the applicability of any exemptions. See 5 U.S.C. § 552(a)(4)(B) (“On complaint, the district court of the United States . . . has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant.”). Under this Circuit’s recent opinion in *Judicial Watch*, the answer to this critical question as to NSPD 54 is no, rendering all other arguments about the applicability of Exemption 5 moot.

The test for whether a record is an “agency record” for the purposes of the FOIA is whether an agency (1) “either create[s] or obtain[s]” the record and (2) is “in control of the requested materials at the time the FOIA request is made.” *U.S. Dep’t of Justice v. Tax Analysts*,

(D.C. Cir. 2008)). Thus, even though the parties have not raised this issue, the Court is obligated to determine, *sua sponte*, whether the records in dispute are “agency records.”

⁶ Exemption 5 incorporates standard discovery privileges which would normally exempt documents from production in the course of civil litigation. See *NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 148–49 (1975). The “presidential communications privilege” is one of those discovery privileges incorporated into Exemption 5. See *Judicial Watch*, 726 F.3d at 229 n.25 (quoting *Baker & Hostetler LLP v. U.S. Dep’t of Commerce*, 473 F.3d 312, 321 (D.C. Cir. 2006)); *Citizens for Responsibility and Ethics in Wash. v. U.S. Dep’t of Homeland Sec.*, 532 F.3d 860, 865 (D.C. Cir. 2008).

492 U.S. 136, 144–45 (1989). The defendant has admitted that it “obtained” NSPD 54. *See* Janosek Decl. ¶ 31 (“[NSPD 54] was issued to a number of high ranking Presidential advisers, Cabinet officials, and agency heads including (*inter alia*) the Director of the NSA.”); Def.’s Mem. in Opp’n to Pl.’s Cross-Mot. Summ. J. and Reply in Supp. of Def.’s Mot. Summ. J. (“Def.’s Reply”) at 17, ECF No. 16 (“NSA has possession of a copy of NSPD 54”). Thus, the first prong of the *Tax Analysts* test is met. Yet, “each [prong] must be satisfied for requested materials to qualify as agency records.” *Tax Analysts*, 492 U.S. at 144. The second, “control” prong is ultimately fatal to the plaintiff’s request.

Judicial Watch established that records originating with the President are subject to the modified “control” test set forth in *United We Stand*, which had previously only been applied to records originating with Congress. *See* 726 F.3d at 224. Under this “control” test, a record is under the control of an agency, thus making it an “agency record,” if the agency has the “ability to use or dispose of the record as it sees fit.” *United We Stand*, 359 F.3d at 600. At issue in *Judicial Watch* were the “official visitors logs and/or other records concerning visits to the White House” for a specified period of time. *Judicial Watch*, 726 F.3d at 214. The D.C. Circuit found that the logs were in the possession of the United States Secret Service, meaning it “obtained” them, but the Secret Service could “use the records for only two limited purposes” and had to transfer the records to the White House and purge them from its computer systems after sixty days. *Id.* at 218–19. The court found that because the White House, an entity not subject to the FOIA, “has manifested its intent to control the entirety of the [visitors logs],” the *United We Stand* test’s application militated against a finding that the logs were “agency records” under the FOIA. *See id.* at 223–24.

As applied to the instant case, the parties do not dispute that NSPD 54 originated with the President or the NSC. *See* Janosek Decl. ¶ 30 (“This document did not originate with NSA, but rather, it originated with the National Security Council (NSC) and Homeland Security Council (HSC).”); Pl.’s Mem. at 3 (“President George W. Bush issued NSPD 54, but did not release the text of the directive to the public.”). The law in this Circuit is clear that the NSC is not an “agency” for the purposes of the FOIA. *See Armstrong v. Exec. Office of the President*, 90 F.3d 553, 559 (D.C. Cir. 1996) *cert. denied* 520 U.S. 1239 (1997); *see also Elec. Privacy Info. Ctr. v. NSA*, 795 F. Supp. 2d 85, 91 (D.D.C. 2011). This is so because the NSC is similar to “the President’s immediate personal staff or units in the Executive Office whose sole function is to advise and assist the President,” which the Supreme Court has held are not an “agency” for the purposes of the FOIA. *See Kissinger v. Reporters Comm. for Freedom of the Press*, 445 U.S. 136, 155 (1980). Indeed, in *Kissinger*, the Supreme Court found that papers and notes generated by the future Secretary of State were not “agency records” because they were created while he was functioning as “Assistant to the President.” *Id.* at 156.

The parties also do not dispute that the President placed significant limits on the distribution of NSPD 54. *See* Janosek Decl. ¶ 31; Pl.’s Mem. at 3; *see also* Ronan Decl. ¶ 7 (“The directive was originally accompanied by a transmittal memo from a Special Assistant to the President . . . [that] emphasized NSPD-54’s close-hold nature and the need to safeguard its content, a need that continues to this day.”). For instance, only specific, high-ranking Presidential advisors were given the directive, and they themselves could only distribute the directive to those within their agencies with a “need to know.” Janosek Decl. ¶¶ 32–33. Indeed, the defendant’s declarant notes that “[e]xplicit White House permission is further required before redistributing NSPD-54 to overseas organizations within the Agency or to other Governmental

agencies/organizations,” *id.* ¶ 33, and the memorandum accompanying NSPD 54 “makes explicitly clear that a recipient of NSPD 54 *should not* distribute or disclose the document without express permission from the White House.” *Id.* ¶ 32 (emphasis in original).

In assessing the level of control exercised by a FOIA-exempt entity, such as Congress or the Office of the President, the D.C. Circuit has considered several indicia. In *Goland v. CIA*, 607 F.2d 339 (D.C. Cir. 1978), the D.C. Circuit rejected a plaintiff’s argument that a classified transcript of a hearing before Congress in the CIA’s possession was an “agency record” merely because it was in the CIA’s possession. *See Goland*, 607 F.2d at 343, 345. The court elaborated that, notwithstanding an agency’s possession, courts must look to whether a FOIA-exempt entity retains control of the document. *See id.* at 345–47. The court found that because, when the CIA received the document, it “bore the typewritten marking ‘Secret’ on its interior cover page,” and that the CIA “retains a copy of the Transcript for internal reference purposes only, to be used in conjunction with legislation concerning the Agency and its operations,” “Congress’ intent to retain control of the document is clear.” *Id.* at 347–48. The court added that “[i]n ascertaining whether a record in the possession of an agency is nonetheless a congressional document, a court will of course accord due weight to the factors that influence us in this case, including (1) Congress’ clear intent to exempt congressional documents from disclosure under FOIA; (2) Congress’ clear prerogative to prevent disclosure of its own confidential materials; and (3) the danger of inhibiting the legislative and judicial branches from making their records available to the executive branch.” *Id.* at 348 n.48.

Similarly, in *United We Stand*, the D.C. Circuit found that a letter sent to the IRS by the congressional Joint Committee on Taxation was not an “agency record” because the document itself stated: “This document is a Congressional record and is entrusted to the Internal Revenue

Service for your use only. This document may not be disclosed without the prior approval of the Joint Committee.” *United We Stand*, 359 F.3d at 600–01. The court went on to find that the agency’s response to the letter must be released under the FOIA as an agency record, with portions redacted so as not to disclose the nature of Congress’ request. *Id.* at 602–03.

By contrast, where the FOIA-exempt entity has conveyed documents to an agency without clear limits on their use or further dissemination, the D.C. Circuit has found the records to be under agency control. In *Holy Spirit Association for the Unification of World Christianity v. CIA*, 636 F.2d 838 (D.C. Cir. 1980) (“*Holy Spirit*”), thirty-five documents containing “correspondence and memoranda originated by one of four congressional committees that investigated various aspects of Korean-American relations between 1976 and 1978” were requested under the FOIA from the CIA, which had possession of the documents. 636 F.2d at 840, *vacated in part on other grounds by* 455 U.S. 997 (1982). The court contrasted the treatment of the requested records with the treatment of three “sealed cartons of additional congressional documents” transferred to the CIA “for safekeeping” at around the same time that were “accompanied by a memorandum from the House Committee on International Relations indicating that the Committee retained jurisdiction over the documents, that the documents contained classified information, and that access to the files was limited to those with authorization from the Clerk of the House.” *Id.* at 842. Unlike the three sealed cartons of documents, the thirty-five records at issue in *Holy Spirit* were not accompanied by any instructions and the agency’s declarant made “clear that only some congressional documents transferred to the CIA contain classified information or details of intelligence activities.” *Id.* at 841–42. The court found that the thirty-five records released to the CIA by Congress without “some clear assertion of congressional control . . . either in the circumstances of the documents’

creation or in the conditions under which they were sent to the CIA” were “agency records” for the purposes of the FOIA. *Id.* at 842.

Likewise, in *Paisley v. CIA*, 712 F.2d 686 (D.C. Cir. 1983), the D.C. Circuit found that documents transferred from the Senate Select Committee on Intelligence to the FBI and CIA pertaining to the shooting death of a former employee were “agency records” because the Committee “affixed no external indicia of control of confidentiality on the faces of the documents,” nor were the “transcripts of testimony [contained in the documents] conducted under any special conditions of secrecy.” *Paisley*, 712 F.2d at 694. Additionally, the court found that even letters from the Committee to the agencies at issue indicating “the Committee’s desire to prevent [the documents’] release without its approval” were insufficient to indicate that Congress retained control because they were “too general and sweeping to provide sufficient proof, when standing alone, of a specific intent to transfer these five . . . documents to the FBI and the CIA for a ‘limited purpose and on condition of secrecy.’” *Id.* at 695 (quoting *Goland*, 607 F.2d at 348 n.48).

Thus, for the purposes of determining the indicia of control evidenced by the FOIA-exempt entity, the D.C. Circuit has consistently looked to the intent of the entity manifested at the time of transfer and the clarity of that intent with respect to the documents subject to the FOIA request.

The D.C. Circuit in *Judicial Watch*, in applying the *United We Stand* control test to the Office of the President, found that “the indicia of White House control in [*Judicial Watch*] are even stronger than the indicia of congressional control in *United We Stand*.” *Judicial Watch*, 726 F.3d at 223. By contrast to the indicia in *United We Stand*, where Congress had asserted only a “limited scope of confidentiality and hence asserted control over only a limited subset of

documents,” the White House in *Judicial Watch* had “manifested its intent to control the entirety of the [visitors logs at issue], all of which it expects the Secret Service to transfer to it.” *Id.* That control was manifested by, *inter alia*, the signing of a Memorandum of Understanding between the White House and the Secret Service instructing that the logs were to be used “for two limited purposes,”⁷ and were to be transferred to the White House and erased from the Secret Service’s computer servers every sixty days. *See id.* at 212. The Memorandum of Understanding also expressly provided that “[a]ny information provided to the Secret Service for the creation of [the logs] is provided under an express reservation of White House control.” *Id.* at 223 (internal quotation marks omitted).

In the instant case, *Judicial Watch* applies *a fortiori*. The White House has manifested its intent to control the entirety of NSPD 54 and its dissemination even within agencies to which the document was distributed, *see* Janosek Decl. ¶ 33, a level of control not present in *Judicial Watch*. Similar to the records in *United We Stand* and *Goland*, NSPD 54 was distributed to agencies with an accompanying memorandum that “forbids . . . intra-agency distribution except on a need to know basis,” and directs that “all public requests for disclosure of NSPD-54” be referred to the NSC and Homeland Security Council (“HSC”). Janosek Decl. ¶¶ 32–33. Indeed, the memorandum made clear that “a recipient of NSPD 54 *should not* distribute or disclose the document without the express permission of the White House.” *Id.* ¶ 32 (emphasis in original). NSPD 54 is decidedly unlike the agency-controlled documents in *Paisley* and *Holy Spirit*, where the FOIA-exempt entity, Congress, placed little or no restrictions on the documents once they were transferred to the agencies. Thus, under the *United We Stand* test, the defendant has shown a sufficiently “clear . . . expression of [White House] intent to control” NSPD 54, making it a

⁷ The Secret Service was only to use the logs to “perform a background check on the visitor, and to verify the visitor’s admissibility at the time of the visit.” *Judicial Watch*, 726 F.3d at 212.

non-agency record for the purposes of the FOIA.⁸ *See* 5 U.S.C. 552(a)(4)(B). Consequently, as it pertains to NSPD 54, summary judgment is granted to the defendant and denied to the plaintiff.

B. Application Of Exemption 5 To NSPDs And Their Predecessors

Although the Court finds that NSPD 54 is not an agency record under the changed legal landscape created by *Judicial Watch*, the determination not to release a NSPD is consistent with the few FOIA cases to have previously addressed this issue. It is first necessary to briefly describe the history of these national security records before discussing the way they have been addressed in prior court decisions.

1. National Security Instruments

NSPD 54 is an example of a type of national security document that began with the formation of the NSC in 1947. *See* HAROLD C. RELYEA, CONG. RESEARCH SERV., CRS NO. 98-611, PRESIDENTIAL DIRECTIVES: BACKGROUND AND OVERVIEW at CRS-8 (2007) (“PRESIDENTIAL DIRECTIVES”). What started as “policy papers” prepared by the NSC’s members and staff eventually became documents signed by the President mandating operating policy. *Id.* at CRS-

⁸ The impact of *Judicial Watch* remains unclear regarding the extent to which the President may make policy decisions and issue directives to Executive branch agencies outside the public eye and beyond the reach of the FOIA, which “is broadly conceived . . . to permit access to official information long shielded unnecessarily from public view . . . [with] a judicially enforceable public right to secure such information from possibly unwilling official hands.” *See Rose*, 425 U.S. at 361. The plaintiff argues convincingly for narrowly construing the scope of Exemption 5 and the presidential communications privilege because “the public will be directly affected by the exercise of the government’s authority” embodied in NSPD 54. Pl.’s Mem. at 21; *id.* at 13–14; *see also Judicial Watch, Inc. v. U.S. Dep’t of Justice*, 365 F.3d 1108, 1116 (D.C. Cir. 2004) (noting the D.C. Circuit has “caution[ed] against the dangers of expanding to a large swath of the executive branch a privilege that is bottomed on a recognition of the unique role of the President”) (quoting *In re Sealed Case*, 121 F.3d 729, 752 (D.C. Cir. 1997) (internal quotation marks omitted)). As the instant case demonstrates, however, under *Judicial Watch*, a President need not invoke the presidential communications privilege—or any other enumerated exemption—to avoid disclosure pursuant to the FOIA of records for which he or she has clearly exerted efforts to retain control and limit dissemination “in the course of” “the carrying out of the constitutional, statutory, official [and] ceremonial duties of the President.” *Judicial Watch*, 726 F.3d at 228 (quoting the definition of “Presidential records” in the Presidential Records Act, 44 U.S.C. § 2201(2)). This result is difficult to reconcile with the D.C. Circuit’s rejection in *Citizens for Responsibility and Ethics in Washington v. United States Department of Homeland Security*, 532 F.3d 860 (D.C. Cir. 2008), of the idea that “the President should *never* have to assert executive privilege in the Exemption 5 context because doing so is simply too burdensome” noting that “can’t be right.” 532 F.3d at 867 (emphasis in original). Nevertheless, *Judicial Watch* appears to create an alternative mechanism for the President to keep records secret without resorting to a FOIA exemption.

8–9. “In general, they were not required to be published in the *Federal Register*, were usually security classified at the highest level of protection, and were available to the public after a great many years had elapsed, usually at the official library of the President who had approved them.” *Id.* at CRS-9.

These national security documents have been known by a series of titles as different Presidents have called them by different names, including NSC Policy Papers, National Security Action Memoranda, National Security Study Memoranda, Presidential Review Memoranda, and Presidential Decision Directives. *Id.* at CRS-9–11. President George W. Bush referred to them as National Security Presidential Directives. *Id.* at CRS-12. The secretive nature of these documents is made apparent by the fact that the public only learns of them once they are released and can only guess at how many each President has issued. *See id.* at CRS-11 (“While the number of NSDs issued by President [George H.W.] Bush remains officially secret, an October 21, 1991, directive concerning single scope security background investigations was designated NSD-63.”). All of them are generated and controlled by the President and NSC staff. *Id.* at CRS-9–12.⁹

2. *National Security Instruments In The Courts*

This is not to say, however, that no NSC directives have ever been released to the public. For instance, in *Los Angeles Times Communications LLC v. United States Department of the Army*, 442 F. Supp. 2d 880 (C.D. Cal. 2006), the Department of the Army included a copy of a

⁹ The plaintiff makes an appealing, but ultimately unavailing, argument that allowing the withholding of NSPD 54 under an expansive view of the presidential communications privilege would allow “documents that will have significant and wide-spread impact [to] be kept totally hidden” and “bring about the very dangers” of “allow[ing] for the creation of ‘secret law,’ the very thing that the FOIA seeks to prevent.” Pl.’s Mem. at 15; *see also* Pl.’s Reply at 10 (“By labeling NSPD 54 a simple ‘communication,’ the NSA mischaracterizes the significance of the document and would encourage expansion of secret law.”). Indeed, the D.C. Circuit has cautioned that Congress “indicated unequivocally that the purpose of [FOIA] was to forbid secret law. And substantive declarations of policy are clearly ‘law’ within the meaning of that prohibition.” *Sterling Drug, Inc. v. FTC*, 450 F.2d 698, 713 (D.C. Cir. 1971) (Bazelon, C.J., concurring in part and dissenting in part) (emphasis in the original). That being said, *Judicial Watch* binds this Court.

NSPD dated May 11, 2004 “regarding United States government operations in Iraq” as part of a declaration in a FOIA case seeking other information about government contractors operating in Iraq. 442 F. Supp. 2d at 891 n.18. Similarly, in *Schreibman v. United States Department of Commerce*, 785 F. Supp. 164 (D.D.C. 1991), the National Institutes of Standards and Technology (“NIST”) provided a copy of a “Presidential directive establishing data security policy and standards” voluntarily in response to a FOIA request. 785 F. Supp. at 165.

By contrast to these examples of voluntary disclosure of Presidential directives, in two cases where FOIA requests directly sought such instruments, the requests were rejected. In *Center for National Security Studies v. Immigration and Naturalization Service*, No. 87-2068, 1990 WL 236133 (D.D.C. Dec. 19, 1990), the plaintiff sought documents under the FOIA pertaining to the “Alien Border Control Committee,” which was a “multi-agency task force formed to address the identification and removal of suspected alien terrorists” under the Reagan Justice Department. 1990 WL 236133 at *1 (internal quotation marks omitted). Among the responsive documents the Department of Justice located was National Security Decision Directive¹⁰ 207, which the defendant withheld in its entirety under FOIA Exemption 1 for classified documents. *Id.* at *2; *see* 5 U.S.C. § 552(b)(1). Since the plaintiff produced no evidence of bad faith on the part of the defendant in its “predictions of harm” to national security if the Directive were released and because such predictions were “entirely plausible and sufficiently descriptive to substantiate an exemption 1 claim,” the court in *Center for National Security Studies* granted summary judgment to the defendant and did not order release of the Directive. *Id.* at *3.

In *Halperin v. National Security Council*, 452 F. Supp. 47 (D.D.C. 1978), the plaintiff sought disclosure of a “compilation of the number and exact title of each National Security Study

¹⁰ This is the name given to NSC policy papers by President Reagan. *See* PRESIDENTIAL DIRECTIVES at CRS-11.

Memoranda” and “National Security Divisional Memoranda” issued during a specific period of time under the Nixon Administration. *Halperin*, 452 F. Supp. at 48. These lists of national security instruments generated by the Nixon NSC and some of the individual titles on the list were classified as “Secret.” *Id.* at 48–49. The defendant withheld the lists in their entirety under Exemption 1 and Exemption 5 to the FOIA. *Id.* at 49. The court in *Halperin* found that the lists were properly classified and non-segregable under Exemption 1 and granted summary judgment to the defendant. *Id.* at 52. Since the court decided the issue based solely on Exemption 1, it expressly declined to address the applicability of Exemption 5. *Id.* at 49.

These cases indicate that NSPD 54 is the type of document that is generally not ordered disclosed under the FOIA. Such national security instruments appear to have only been released voluntarily by the President or NSC that created them, or their release has been approved after a substantial period of time has passed, typically through Presidential libraries. *See* PRESIDENTIAL DIRECTIVES at CRS-9. Although the plaintiff in the instant case has made strong arguments as to why the public has an interest in the release of NSPD 54, precedent counsels that such documents have not been found releasable under the FOIA.¹¹ In this respect, NSPD 54 is similar in kind to the records at issue in *Judicial Watch*, where the circumstance deemed “most important” in bolstering the conclusion that those White House records were beyond the reach of FOIA, was that the court was “not confronted with an attempt to protect information that would otherwise be subject to FOIA.” 726 F.3d. at 232.

* * *

In *Judicial Watch*, the D.C. Circuit responded to the “fear that this case will open the floodgates to White House efforts to circumvent FOIA,” by clarifying that its holding was not

¹¹ Since NSPD 54 is not an “agency record” for the purposes of the FOIA, the Court does not opine as to whether the presidential communications privilege encompassed in Exemption 5 is coextensive with the privilege as it is asserted in the civil discovery context, as the parties have disputed in their briefing.

that “*any* record touching on White House communications were necessarily exempt from FOIA.” 726 F. 3d at 231 (emphasis in original). The court pointed to three circumstances that limited the application of its holding: first, that “no deference” was given to a Memorandum of Understanding (“MOU”) between the White House and the agency stating that the White House retained “exclusive *legal* custody and control” of the records at issue. *Id.* (emphasis in original). While not acceding to the legal conclusion articulated in the MOU, the court did, however, rely on “the way in which both parties have historically regarded and treated the documents.” *Id.* Similarly, in the instant case, the White House’s explicit instructions regarding the limited use and dissemination of NSPD 54 only with the White House’s approval, appears to satisfy this circumstance showing that the White House took clearly articulated steps to retain control over the document.

The second circumstance cited by the court in *Judicial Watch* as limiting its holding is that potential release of the records at issue under the FOIA would “put the President on the horns of a dilemma between surrendering his confidentiality and jeopardizing his safety,” which the court found to be “comparable to” the “presence of [] unacceptable choice,” faced by Congress in *United We Stand* and *Goland*. *Id.* at 231–32. In *Goland*, the D.C. Circuit noted the conflict between Congress’ “constitutional prerogative of maintaining secrecy” in its communications with agencies over which it “exercises oversight authority” and a finding that any records in possession of an agency are automatically subject to the FOIA, which the D.C. Circuit noted would cause “an impairment of [Congress’] oversight role.” *Goland*, 607 F.2d at 346. In *United We Stand*, where the documents at issue were created by an agency in response to a Congressional request, Congress evinced a clear intent to keep its request to the agency secret as part of “the Joint Committee[’s] belie[f] that confidentiality is critical to its work.” *United We*

Stand, 359 F.3d at 602. In the instant case, the defendant notes that NSPD 54 requested that “his advisers . . . submit follow-up reports,” Def.’s Mem. at 10, and confidentiality was necessary because the release of NSPD 54 “would ‘limit the President’s ability to communicate his decisions privately, thereby interfering with his ability to exercise control over the executive branch.’” *Id.* (quoting *In re Sealed Case*, 121 F.3d at 745–46). This protection of confidentiality and the President’s role in overseeing executive agencies is the same type of conflict the D.C. Circuit was concerned with in *Goland*, *United We Stand*, and *Judicial Watch*.

Finally, the last circumstance, deemed to be the “most important,” limitation on the *Judicial Watch* holding is that the requested records “involves a category of documents that effectively reproduces a set of records that Congress expressly excluded from FOIA’s coverage,” *id.* at 232, as detailed in the legislative history for the 1974 FOIA amendments, *id.* at 224–25 (discussing the Conference Report, which stated that the definition of an “agency” subject to FOIA does not include the Office of the President or the President’s immediate personal staff or units in the Executive Office whose sole function is to advise and assist the President). The White House visitor logs at issue in *Judicial Watch* “would not even arguably be subject to the Act, but for the President’s need for Secret Service protection.” *Id.* at 232. Thus, the necessity of sharing with agents of the Secret Service the otherwise FOIA-exempt White House visitor requests did not pierce the confidentiality that the President was otherwise entitled to enjoy in those records. Similarly, here, the necessity of the President of communicating to a limited group of high-ranking Executive branch officials any instructions and guidance contained in NSPD 54 in order to effectuate the President “carrying out the constitutional, statutory, or other official or ceremonial duties of the President,” appears to fall squarely within the same category of documents found to be outside the reach of FOIA in *Judicial Watch*. Indeed, the question in

Judicial Watch appears to be a closer one than the question here, as the documents in *Judicial Watch* were created by an agency subject to the FOIA, namely, the Secret Service, whereas in the instant case NSPD 54 was created by a FOIA-exempt entity itself, namely, the NSC, and merely distributed to agencies subject to the FOIA.

In short, none of the limitations on the holding in *Judicial Watch* appear to distinguish this case or make inapplicable the control test now required in determining whether NSPD 54 is an “agency record.”

C. The Defendant Properly Asserted Exemption 1 As To The Remaining Documents

The plaintiff challenges the defendant’s redaction of IAD Management Directive 20 and NSA/CSS Policy 1-58 under Exemption 1 to the FOIA, which provides that records “specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and . . . are in fact properly classified pursuant to such Executive order” are exempt from mandatory disclosure under the FOIA. 5 U.S.C. § 552(b)(1)(A–B). The plaintiff argues that “the agency has not established that NSPD 54 and the related records are properly classified.” Pl.’s Mem. at 22. As discussed in Part III.A, NSPD 54 is a non-agency record and not covered by the FOIA. Since the remaining two documents did not originate with a FOIA-exempt entity and are “agency records,” the defendant bears the burden of showing that they were appropriately redacted. *See Assassination Archives & Research Ctr.*, 334 F.3d at 57 (D.C. Cir. 2003).

The plaintiff’s challenge to the withheld portions consists of a conclusory statement that “[t]he NSA presents no evidence that Ms. Ronan and Ms. Janosek have been delegated classification authority by the President or Vice President, or an agency head that was first delegated such authority by the President or Vice President” as required by Executive Order

13526 to confer classification authority. Pl.’s Mem. at 24. This challenge fails to address the unequivocal statement by both declarants that they have been delegated classification authority under Executive Order 13526. *See* Ronan Decl. ¶ 1; Janosek Decl. ¶ 20. The plaintiff has offered no evidence to cast doubt upon these sworn declarations.

In reviewing withholdings under Exemption 1, “courts must accord *substantial* weight to an agency’s affidavit concerning the details of the classified status of the disputed record.” *Wolf*, 473 F.3d at 374 (quoting *Miller v. Casey*, 730 F.2d 773, 776 (D.C. Cir. 1984)) (emphasis in original, internal quotation marks omitted). When provided with an affidavit that “describe[s] the justifications for nondisclosure with reasonably specific detail, demonstrate[s] that the information withheld logically falls within the claimed exemption, and [is] not controverted by either contrary evidence in the record nor by evidence of agency bad faith,” summary judgment is warranted for the agency. *Miller*, 730 F.2d at 776 (internal quotation marks and citations omitted). Here, the plaintiff does not challenge the agency’s purported justification for the classification, but rather that the individual declarants did not have adequate classification authority. *See* Pl.’s Mem. at 23–24. Considering the substantial deference the Court must show to agency declarations when Exemption 1 is claimed, and in the absence of any evidence other than a bald assertion that the declarants have not proven that they are valid classification authorities, despite their sworn affidavits to the contrary, the Court grants summary judgment to the defendant on its Exemption 1 withholdings in IAD Management Directive 20 and NSA/CSS Policy 1-58.¹²

¹² To the extent the plaintiff challenges the defendant’s withholdings under Exemption 3, the plaintiff’s argument is entirely predicated upon the fact that the “records described . . . are not properly classified.” *See* Pl.’s Mem. at 25. Since the Court has found the plaintiff’s argument on that score to be unpersuasive, the plaintiff’s Exemption 3 argument is similarly unavailing.

D. The Defendant Construed The Plaintiff's FOIA Request Too Narrowly

Finally, the plaintiff argues that the defendant's "interpretation of [the plaintiff's] plainly worded FOIA Request is contrary to the FOIA and relevant case law." In essence, the plaintiff argues that the defendant improperly narrowed its search when responding to the second part of the plaintiff's requests to search only for records distributed "to the NSA" rather than "to any federal agency charged with implementing the cybersecurity scheme," as stated in the plaintiff's request. Pl.'s Reply Supp. Pl.'s Cross-Mot. Summ. J. ("Pl.'s Reply") at 12, ECF No. 17; *see also* Janosek Decl. Tab A at 5. The defendant's declarant gives credence to the plaintiff's argument, as the Janosek Declaration notes the defendant "searched for responsive records by giving plain meaning to Plaintiff's request and thus searched for 'Executing protocols' that were 'distributed to' to [sic] the NSA – meaning, protocols that emanated from outside the NSA and were 'distributed to' NSA." Janosek Decl. ¶ 36.

The plaintiff's request sought "the full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to *the agencies in charge of its implementation*." Janosek Decl. Tab A at 5 (emphasis added). There is no dispute that the defendant is one of the agencies "in charge of" the CNCI's implementation, and, consequently, the agency's search for pertinent records "distributed to the NSA" fell within the request's parameters. Yet, the plaintiff is correct that the defendant "may be in possession of the CNCI or related records that were issued to the FBI, the CIA, or other federal agencies," either by an entity other than the defendant or by the defendant itself. *See* Pl.'s Reply at 12. Such documents, under the plain meaning of the plaintiff's FOIA request, are responsive to the request.¹³

¹³ The plaintiff also asserts that NSPD 54 is responsive to the second part of the plaintiff's FOIA request and therefore should have been deemed a responsive record to this portion of the request. *See* Pl.'s Mem. at 26. The

The plaintiff is correct that “an agency . . . has a duty to construe a FOIA request liberally.” *Nation Magazine v. U.S. Customs Serv.*, 71 F.3d 885, 890 (D.C. Cir. 1995). By limiting its interpretation of records responsive to the plaintiff’s requests only to records emanating from outside the defendant agency, the defendant violates this basic FOIA convention. If the defendant itself generated an executing protocol for the CNCI and distributed it to other relevant federal agencies, those records were “distributed to the agencies in charge of [the CNCI’s] implementation.”

Notably, the plaintiff is not asserting that the defendant performed an inadequate search for responsive records. *See* Pl.’s Mem. at 27 (“[The plaintiff] has not challenged, and does not purport to challenge here, the sufficiency of the [defendant’s] search for agency records.”). Instead, the plaintiff is arguing that the defendant “searched for, located, reviewed, but unlawfully withheld as ‘unresponsive’ records that are responsive to Category 2 of [the plaintiff’s] FOIA Request.” *Id.* Thus, the defendant is directed to produce to the plaintiff records discovered responsive to the second part of the plaintiff’s request, including executing protocols in the defendant’s possession that were distributed to other relevant federal agencies, that were received by the NSA or distributed by the NSA, unless those records are properly withheld, in whole or in part, under exemptions to the FOIA.

IV. CONCLUSION

The primary document at issue here, NSPD 54, is not an agency record for the purposes of the FOIA under the *Judicial Watch* standard and therefore need not be disclosed in response to a FOIA request. In addition, the plaintiff’s challenges to the defendant’s redactions of IAD

defendant admits as much, Def.’s Reply at 17, but, as discussed *supra*, this document is properly withheld because it is not an “agency record” for the purposes of the FOIA. Thus, the plaintiff’s argument that NSPD 54 is responsive to the second portion of its request if it were an “agency record” is technically correct, but does not yield a different result.

Management Directive 20 and NSA/CSS 1-58 under Exemptions 1 and 3 are rejected. The plaintiff is correct, however, that the defendant improperly narrowed its search for responsive records to the second portion of the plaintiff's FOIA requests to only those records distributed to the NSA, rather than to all agencies charged with implementing the CNCI. Consequently, the defendant's Motion for Summary Judgment is GRANTED in part and DENIED in part and the plaintiff's Cross-Motion for Summary Judgment is GRANTED in part and DENIED in part. The defendant shall review its search to determine if any records found in that search are responsive to the plaintiff's FOIA request, conforming its interpretation of that request to the instructions of this Court. After such review, the defendant shall supplement its production to the plaintiff with any responsive records or, in the alternative, submit a *Vaughn* index detailing what records or portions of records are being withheld and under what exemptions to the FOIA. The parties are instructed to jointly file a briefing schedule to facilitate the timely production of these documents and resolution of any disputes which may arise regarding their production.

An appropriate Order will accompany this Memorandum Opinion.

Date: October 21, 2013



Digitally signed by Beryl A. Howell
DN: cn=Beryl A. Howell, o=District
Court for the District of Columbia,
ou=District Court Judge,
email=howell_chambers@dcd.uscourts
.gov, c=US
Date: 2013.10.21 17:08:33 -0400

BERYL A. HOWELL
United States District Judge

**U.S. District Court
 District of Columbia (Washington, DC)
 CIVIL DOCKET FOR CASE #: 1:10-cv-00196-BAH**

ELECTRONIC PRIVACY INFORMATION CENTER v.
 NATIONAL SECURITY AGENCY et al
 Assigned to: Judge Beryl A. Howell
 Case in other court: USCA, 13-05369
 Cause: 05:552 Freedom of Information Act

Date Filed: 02/04/2010
 Date Terminated: 11/19/2013
 Jury Demand: None
 Nature of Suit: 895 Freedom of
 Information Act
 Jurisdiction: U.S. Government Defendant

Date Filed	#	Docket Text
02/04/2010	<u>1</u>	COMPLAINT against NATIONAL SECURITY AGENCY, NATIONAL SECURITY COUNCIL (Filing fee \$ 350, receipt number 4616027382) filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # <u>1</u> Civil Cover Sheet)(rdj) (Entered: 02/05/2010)
02/04/2010		SUMMONS (4) Issued as to NATIONAL SECURITY AGENCY, NATIONAL SECURITY COUNCIL, U.S. Attorney and U.S. Attorney General (rdj) (Entered: 02/05/2010)
02/04/2010	<u>2</u>	LCvR 7.1 CERTIFICATE OF DISCLOSURE of Corporate Affiliations and Financial Interests by ELECTRONIC PRIVACY INFORMATION CENTER identifying Corporate Parent NONE for ELECTRONIC PRIVACY INFORMATION CENTER. (rdj) (Entered: 02/05/2010)
03/25/2010	<u>3</u>	NOTICE of Appearance by Joshua Ilan Wilkenfeld on behalf of NATIONAL SECURITY AGENCY, NATIONAL SECURITY COUNCIL (Wilkenfeld, Joshua) (Entered: 03/25/2010)
03/25/2010	<u>4</u>	MOTION to Dismiss <i>Partial Motion to Dismiss</i> by NATIONAL SECURITY AGENCY, NATIONAL SECURITY COUNCIL (Attachments: # <u>1</u> Text of Proposed Order)(Wilkenfeld, Joshua) (Entered: 03/25/2010)
03/25/2010	<u>5</u>	ANSWER to <u>1</u> Complaint by NATIONAL SECURITY AGENCY.(Wilkenfeld, Joshua) (Entered: 03/25/2010)
03/25/2010	<u>6</u>	STANDING ORDER Signed by Judge Ricardo M. Urbina on 3/25/2010. Read this Standing Order carefully, it will govern this case. Failure to follow the Standing Order will result in sanctions.(tg,) (Entered: 03/25/2010)
04/08/2010	<u>7</u>	Memorandum in opposition to re <u>4</u> MOTION to Dismiss <i>Partial Motion to Dismiss</i> filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # <u>1</u> Text of Proposed Order)(Verdi, John) (Entered: 04/08/2010)
04/15/2010	<u>8</u>	REPLY to opposition to motion re <u>4</u> MOTION to Dismiss <i>Partial Motion to Dismiss</i> filed by NATIONAL SECURITY AGENCY, NATIONAL SECURITY COUNCIL. (Wilkenfeld, Joshua) (Entered: 04/15/2010)
01/20/2011		Case reassigned to U.S. District Judge Beryl A. Howell. Judge Ricardo M. Urbina no longer assigned to the case. (gt,) (Entered: 01/20/2011)
07/07/2011	<u>9</u>	MEMORANDUM OPINION regarding <u>4</u> defendants' partial motion to dismiss. Signed by Judge Beryl A. Howell on 7/7/2011. (lcbah2) (Entered: 07/07/2011)
07/07/2011	<u>10</u>	ORDER granting <u>4</u> Defendants' Partial Motion to Dismiss for the reasons set forth in the accompanying Memorandum Opinion. Signed by Judge Beryl A. Howell on 7/7/2011. (lcbah2) (Entered: 07/07/2011)
07/07/2011		Set/Reset Deadlines: Joint Report due by 7/20/2011. (zalg,) (Entered: 07/08/2011)
07/20/2011	<u>11</u>	STATUS REPORT <i>JOINT REPORT</i> by ELECTRONIC PRIVACY INFORMATION CENTER, NATIONAL SECURITY AGENCY. (Wilkenfeld, Joshua) (Entered: 07/20/2011)

07/21/2011		MINUTE ORDER (paperless) adopting the following proposed SCHEDULING ORDER: The last day for supplemental production of responsive documents shall be August 30, 2011. Defendant's motion for summary judgment and supporting materials shall be filed by October 11, 2011. Plaintiff's cross-motion for summary judgment and opposition to defendant's motion for summary judgment shall be filed by November 11, 2011. Defendant's reply in further support of its motion and opposition to plaintiff's cross-motion shall be filed by December 8, 2011. Plaintiff's reply in further support of its cross-motion shall be filed by December 22, 2011. Signed by Judge Beryl A. Howell on 7/21/2011. (lcbah2) (Entered: 07/21/2011)
07/21/2011		Set/Reset Deadlines: Supplemental production of responsive documents shall be filed by 8/30/11. Defendant's motion for summary judgment and supporting materials shall be filed by 10/11/11. Plaintiff's cross-motion for summary judgment and opposition to defendant's motion for summary judgment shall be filed by 11/11/11. Defendant's reply in further support of its motion and opposition to plaintiff's cross-motion shall be filed by 12/8/11. Plaintiff's reply in further support of its cross-motion shall be filed by 12/22/11. (zalg,) (Entered: 07/26/2011)
10/11/2011	<u>12</u>	MOTION for Summary Judgment by NATIONAL SECURITY AGENCY (Attachments: # <u>1</u> Memorandum in Support, # <u>2</u> Declaration Declaration of Diane M. Janosek, # <u>3</u> Tab A, # <u>4</u> Tab B, # <u>5</u> Tab C, # <u>6</u> Tab D, # <u>7</u> Tab E, # <u>8</u> Tab F, # <u>9</u> Tab G, # <u>10</u> Declaration Declaration of Mary Ronan, # <u>11</u> Statement of Facts, # <u>12</u> Text of Proposed Order)(Wilkenfeld, Joshua) (Entered: 10/11/2011)
11/11/2011	<u>13</u>	Cross MOTION for Summary Judgment <i>Combined Cross-Motion and Motion for Oral Hearing</i> by ELECTRONIC PRIVACY INFORMATION CENTER (Attachments: # <u>1</u> Memorandum in Support, # <u>2</u> Statement of Facts, # <u>3</u> Statement of Genuine Issues in Opposition to Defendant's Statment of Material Facts, # <u>4</u> Text of Proposed Order)(Verdi, John). Added MOTION for Hearing on 11/14/2011 (jf,). (Entered: 11/11/2011)
11/11/2011	<u>14</u>	Memorandum in opposition to re <u>12</u> MOTION for Summary Judgment <i>Combined Cross-Motion and Opposition</i> filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Attachments: # <u>1</u> Statement of Facts, # <u>2</u> Statement of Genuine Issues in Opposition to Defendant's Statement of Material Facts, # <u>3</u> Text of Proposed Order)(Verdi, John) (Entered: 11/11/2011)
12/08/2011	<u>15</u>	REPLY to opposition to motion re <u>12</u> MOTION for Summary Judgment filed by NATIONAL SECURITY AGENCY. (Attachments: # <u>1</u> Statement of Genuine Issues in Opposition to Plaintiff's Statement of Material Facts)(Wilkenfeld, Joshua) (Entered: 12/08/2011)
12/08/2011	<u>16</u>	Memorandum in opposition to re <u>13</u> Cross MOTION for Summary Judgment <i>Combined Cross-Motion and Opposition</i> MOTION for Hearing <i>Combined reply in support of NSA's motion for summary judgment and opposition to Plaintiff's cross-motion for summary judgment</i> filed by NATIONAL SECURITY AGENCY. (Attachments: # <u>1</u> Statement of Genuine Issues in Opposition to Plaintiff's Statement of Material Facts)(Wilkenfeld, Joshua) (Entered: 12/08/2011)
12/22/2011	<u>17</u>	REPLY to opposition to motion re <u>13</u> Cross MOTION for Summary Judgment <i>Combined Cross-Motion and Opposition</i> MOTION for Hearing filed by ELECTRONIC PRIVACY INFORMATION CENTER. (Verdi, John) (Entered: 12/22/2011)
03/28/2012	<u>18</u>	NOTICE of Appearance by Marc Rotenberg on behalf of ELECTRONIC PRIVACY INFORMATION CENTER (Rotenberg, Marc) (Entered: 03/28/2012)
03/28/2012	<u>19</u>	NOTICE OF WITHDRAWAL OF APPEARANCE as to ELECTRONIC PRIVACY INFORMATION CENTER. Attorney John Arthur Verdi terminated. (Verdi, John) (Entered: 03/28/2012)
05/22/2012	<u>20</u>	NOTICE OF SUBSTITUTION OF COUNSEL by Judson Owen Littleton on behalf of NATIONAL SECURITY AGENCY Substituting for attorney Joshua Wilkenfeld (Littleton, Judson) (Entered: 05/22/2012)

Date	Page	Description
10/10/2012	<u>21</u>	NOTICE of Appearance by Ginger P. McCall on behalf of ELECTRONIC PRIVACY INFORMATION CENTER (McCall, Ginger) (Entered: 10/10/2012)
12/22/2012	<u>22</u>	STATUS REPORT by ELECTRONIC PRIVACY INFORMATION CENTER. (Rotenberg, Marc) (Entered: 12/22/2012)
07/08/2013	<u>23</u>	NOTICE OF SUBSTITUTION OF COUNSEL by Gregory Peter Dworkowitz on behalf of NATIONAL SECURITY AGENCY Substituting for attorney Judson O. Littleton (Dworkowitz, Gregory) (Entered: 07/08/2013)
08/02/2013	<u>24</u>	NOTICE OF WITHDRAWAL OF APPEARANCE as to ELECTRONIC PRIVACY INFORMATION CENTER. Attorney Ginger P. McCall terminated. (McCall, Ginger) (Entered: 08/02/2013)
09/09/2013		MINUTE ORDER (paperless) Pending before the Court are the <u>12</u> Defendant's Motion for Summary Judgment and the <u>13</u> Plaintiff's Cross-Motion for Summary Judgment, in which the parties dispute whether the "National Security Presidential Directive 54 ("NSPD 54") and related agency records," are exempt from disclosure under the Freedom of Information Act ("FOIA"). The parties assume in their briefing that the requested documents are "agency records" subject to FOIA disclosure, unless one of nine specific exemptions applies. See 5 U.S.C. § 552(b)(1)-(9); Pl's Mem. in Supp. of Cross-Mot. for Summ. J ("Pl's Mem.") at 2, ECF No. 13-1; Def's Mem. in Supp. of Mot. for Summ. J. ("Def's Mem.") at 3, ECF No. 12-1. In <i>Judicial Watch v. United States Secret Service</i> , Civil No. 11-5282, 2013 U.S. App. LEXIS 18119 (D.C. Cir. August 30, 2013), the United States Court of Appeals for the District of Columbia Circuit determined that certain White House Access Control System ("WHACS") records, which were "arguably created by White House staff... in the course of carrying out the constitutional, statutory, official, and ceremonial duties of the President," <i>id.</i> at 54-55 (internal quotations and citations omitted), were not "agency records" subject to the FOIA. In reaching this conclusion, the D.C. Circuit applied the modified control test set forth in <i>United We Stand America, Inc. v. IRS</i> , 359 F.3d 595 (2004), which had previously been applied only to Congressional records, 2013 U.S. App. LEXIS 18119 at 40-41 n. 21. A critical focus of the modified control test is whether "the non-covered entity here, the White House has manifested a clear intent to control the documents." <i>Id.</i> at 37. If the parties would like the opportunity to address the relevance, if any, of the D.C. Circuit's recent decision in <i>Judicial Watch</i> to the issues raised by the withholding of the requested documents in the instant case, the parties are directed to submit jointly, by September 16, 2013, a schedule for supplemental briefing. Signed by Judge Beryl A. Howell on 09/09/2013. (lcbah2) (Entered: 09/09/2013)
09/09/2013		Set/Reset Deadlines: Joint schedule for supplemental briefing due by 9/16/2013. (tg,) (Entered: 09/09/2013)
09/16/2013	<u>25</u>	NOTICE of Appearance by Amie L. Stepanovich on behalf of ELECTRONIC PRIVACY INFORMATION CENTER (Stepanovich, Amie) (Entered: 09/16/2013)
09/16/2013	<u>26</u>	STATUS REPORT <i>JOINT STATUS REPORT</i> by ELECTRONIC PRIVACY INFORMATION CENTER. (Stepanovich, Amie) (Entered: 09/16/2013)
10/21/2013	<u>27</u>	MEMORANDUM AND OPINION regarding the defendant's <u>12</u> Motion for Summary Judgment and the plaintiff's <u>13</u> Cross-Motion for Summary Judgment. Signed by Judge Beryl A. Howell on October 21, 2013. (lcbah1) (Entered: 10/21/2013)
10/21/2013	<u>28</u>	ORDER GRANTING in part and DENYING in part the defendant's <u>12</u> Motion for Summary Judgment; GRANTING in part and DENYING in part the plaintiff's <u>13</u> Motion for Summary Judgment and DENYING the plaintiff's <u>13</u> Motion for Hearing as moot. The parties shall, by November 4, 2013, jointly file a proposed schedule to facilitate the timely production of records responsive to the second portion of the plaintiff's FOIA request and resolution of any disputes which may arise regarding their production. See Order for further details. Signed by Judge Beryl A. Howell on October 21, 2013. (lcbah1,) (Entered: 10/21/2013)
10/22/2013		Set/Reset Deadlines: Response to Order of the Court due by 11/4/2013. (tg,) (Entered: 10/22/2013)

Date	Page	Description
11/04/2013	<u>29</u>	STATUS REPORT <i>JOINT STATUS REPORT</i> by ELECTRONIC PRIVACY INFORMATION CENTER. (Stepanovich, Amie) (Entered: 11/04/2013)
11/04/2013		MINUTE ORDER (paperless) entering the following SCHEDULING ORDER to control further proceedings in this matter. The defendant shall, by November 8, 2013, provide any remaining responsive records to the plaintiff or, in the alternative, submit a Vaughn index detailing the records or portions of records being withheld. The parties shall, by November 15, 2013, jointly file a proposed briefing schedule to resolve any outstanding disputes in this matter or advise the Court that this case should be closed. Signed by Judge Beryl A. Howell on November 4, 2013. (lcbah1) (Entered: 11/04/2013)
11/05/2013		Set/Reset Deadlines: Defendant's Responsive records or in the alternative a Vaughn Index due by 11/8/2013. Joint Briefing Schedule due by 11/15/2013. (tg,) (Entered: 11/05/2013)
11/15/2013	<u>30</u>	STATUS REPORT by ELECTRONIC PRIVACY INFORMATION CENTER. (Stepanovich, Amie) (Entered: 11/15/2013)
11/15/2013		MINUTE ORDER (paperless) CLOSING this matter. In light of the parties' <u>30</u> Joint Status Report, in which the parties state that there "are no further substantive issues to be resolved by this Court," the Clerk is directed to close this case. The Court retains jurisdiction of this matter for the purposes of determining appropriate allocation of fees and costs, if judicial intervention is warranted. The parties are ORDERED to jointly file, by December 16, 2013, a status report indicating whether briefing on fees and costs will be necessary and, if so, a proposed schedule for such briefing. Signed by Judge Beryl A. Howell on November 15, 2013. (lcbah1) (Entered: 11/15/2013)
11/19/2013		Set/Reset Deadlines: Joint Status Report due by 12/16/2013. (tg,) (Entered: 11/19/2013)
12/16/2013	<u>31</u>	STATUS REPORT <i>JOINT STATUS REPORT</i> by ELECTRONIC PRIVACY INFORMATION CENTER. (Stepanovich, Amie) (Entered: 12/16/2013)
12/17/2013		MINUTE ORDER (paperless) DIRECTING the parties, pursuant to their <u>31</u> Joint Status Report, jointly to file, by December 20, 2013, a status report advising the Court whether additional proceedings are necessary in this matter. Signed by Judge Beryl A. Howell on December 17, 2013. (lcbah1) (Entered: 12/17/2013)
12/17/2013		Set/Reset Deadlines: Joint Status Report due by 12/20/2013. (tg,) (Entered: 12/17/2013)
12/17/2013	<u>32</u>	NOTICE OF APPEAL TO DC CIRCUIT COURT as to <u>28</u> Order on Motion for Summary Judgment,, Order on Motion for Hearing,,,,, <u>27</u> Memorandum & Opinion by ELECTRONIC PRIVACY INFORMATION CENTER. Filing fee \$ 505, receipt number 0090-3568134. Fee Status: Fee Paid. Parties have been notified. (Rotenberg, Marc) (Entered: 12/17/2013)
12/18/2013	<u>33</u>	Transmission of the Notice of Appeal, Order Appealed, and Docket Sheet to US Court of Appeals. The Court of Appeals fee was paid this date re <u>32</u> Notice of Appeal to DC Circuit Court. (rdj) (Entered: 12/18/2013)
12/20/2013	<u>34</u>	STATUS REPORT (<i>Joint</i>) by NATIONAL SECURITY AGENCY. (Dworkowitz, Gregory) (Entered: 12/20/2013)
12/23/2013		MINUTE ORDER (paperless) DIRECTING the parties, upon consideration of their <u>34</u> Joint Status Report and the pendency of an appeal in this case, jointly to file, within 30 days of the disposition of the appeal, a status report advising the Court whether additional proceedings are necessary in this matter. Signed by Judge Beryl A. Howell on December 23, 2013. (lcbah1) (Entered: 12/23/2013)
12/24/2013		USCA Case Number 13-5369 for <u>32</u> Notice of Appeal to DC Circuit Court, filed by ELECTRONIC PRIVACY INFORMATION CENTER. (rdj) (Entered: 12/24/2013)
02/03/2014	<u>35</u>	NOTICE OF WITHDRAWAL OF APPEARANCE as to ELECTRONIC PRIVACY INFORMATION CENTER. Attorney Amie L. Stepanovich terminated. (Stepanovich, Amie) (Entered: 02/03/2014)

02/10/2014	<u>36</u>	NOTICE of Acceptance with Offer of Judgment by NATIONAL SECURITY AGENCY (Attachments: # <u>1</u> Exhibit A: Offer of Judgment, # <u>2</u> Exhibit B: Proof of Service)(Dworkowitz, Gregory) (Entered: 02/10/2014)
02/11/2014	<u>37</u>	CLERK'S JUDGMENT ON OFFER AND ACCEPTANCE in favor of ELECTRONIC PRIVACY INFORMATION CENTER against UNITED STATES NATIONAL SECURITY AGENCY (tg.) (Entered: 02/11/2014)

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

FILED
FEB 4, 2010
Clerk, U.S. District and
Bankruptcy Courts

ELECTRONIC PRIVACY INFORMATION CENTER)
1718 Connecticut Ave., N.W.)
Suite 200)
Washington, DC 20009)

Plaintiff,)

v.)

NATIONAL SECURITY AGENCY)
9800 Savage Road)
Ft. George G. Meade, MD 20755-6000)

NATIONAL SECURITY COUNCIL)
Old Executive Office Building)
Washington, DC 20506)

Defendants.)

Case: 1:10-cv-00196
Assigned To : Urbina, Ricardo M.
Assign. Date : 2/4/2010
Description: FOIA/Privacy Act

COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552 (2007), for injunctive and other appropriate relief, seeking the release of agency records requested by the Electronic Privacy Information Center from the United States National Security Agency/Central Security Service.

Jurisdiction and Venue

2. This Court has subject matter jurisdiction over this action and personal jurisdiction over the parties pursuant to 5 U.S.C. § 552(a)(4)(B) (2009), 5 U.S.C. § 552(a)(6)(C)(i) (2009), and 5 U.S.C. § 703 (2009). This Court also has jurisdiction over this action pursuant to 28 U.S.C. § 1331 (2009). Venue is proper in this district under 5 U.S.C. § 552(a)(4)(B) (2009) and 5 U.S.C. § 703 (2009).

1

Parties

3. Plaintiff Electronic Privacy Information Center (“EPIC”) is a public interest research organization incorporated as a not-for-profit corporation in Washington, D.C. EPIC’s activities include the review of federal activities and policies to determine their possible impacts on civil liberties and privacy interests. Among its other activities, EPIC publishes books, reports, and a bi-weekly electronic newsletter. EPIC also maintains a heavily visited Internet site, <http://www.epic.org>, which contains extensive information regarding privacy issues, including information EPIC has obtained from federal agencies under the FOIA.

4. Defendant National Security Agency/Central Security Service (“NSA/CSS,” “NSA,” or “Agency”) is an intelligence agency established in the Executive Branch of the United States Government, administered within the United States Department of Defense. The NSA is an agency within the meaning of 5 U.S.C. § 552(f)(1) (2009).

5. Defendant National Security Council (“NSC”, or “Council”) is a branch of the Executive Office of the President of the United States and exists to advise the President with respect to policies concerning the national security of the United States. The Council’s structure and function are established in 50 U.S.C. § 402 (2009).

Facts

A National Security Presidential Directive has Reshaped National Cybersecurity Policy

6. On January 8, 2008, President George W. Bush issued National Security Presidential Directive 54 (“NSPD 54”), also known as Homeland Security Presidential Directive 23.

7. The contents of NSPD 54 have not been released to the public.

8. NSPD 54 established the Comprehensive National Cybersecurity Initiative

(“CNCI”).

9. On May 1, 2008, Senators Joseph I. Lieberman and Susan M. Collins, Chairman and Ranking Member, respectively, of the United States Senate Committee on Homeland Security and Governmental Affairs, wrote a letter to Michael Chertoff, then Secretary of the United States Department of Homeland Security, regarding the CNCI.

10. According to the May 1, 2008 letter, the CNCI “is a multi-agency, multi-year plan that lays out twelve steps to securing the federal government’s cyber networks.”

11. In a letter dated March 5, 2009, Rod Beckstrom resigned from the position of Director of the National Cybersecurity Center (NCSC) within the Department of Homeland Security.

12. In the March 5, 2009 letter, Beckstrom stated that “NSA currently dominates most national cyber efforts.”

13. The Cybersecurity Act of 2009 (S. 773) was introduced in the Senate on April 1, 2009, by Senator Jay Rockefeller.

14. The Cybersecurity Act of 2009 (S. 773) is currently pending in the Senate Committee on Commerce, Science, and Transportation.

EPIC Submitted a FOIA Request to the NSA Regarding NSPD 54 and the CNCI

15. On June 25, 2009, EPIC transmitted a written FOIA request to the NSA for agency records (“EPIC’s FOIA Request”). EPIC requested the following agency records:

- a. the text of the National Security Presidential Directive 54 otherwise referred to as Homeland Security Presidential Directive 23;
- b. the full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation; and

- c. any privacy policies related to either the Directive, the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative.

16. EPIC also asked the NSA to expedite its responses on the basis that the documents pertain to a matter about which there is an urgency to inform the public about an actual or alleged federal government activity, and the request was made by a person primarily engaged in disseminating information, pursuant to 5 U.S.C. § 552(a)(6)(E) (2009). Petitioner based the request on the public's and press's interest in national cybersecurity policy and CNCI, especially with respect to the pending Cybersecurity Act of 2009.

17. EPIC further requested that all fees be waived based on EPIC's status as a representative of the news media.

18. EPIC's FOIA Request was transmitted by facsimile to the NSA at (443) 479-3612. EPIC received an automated facsimile statement confirming the NSA's receipt of the transmittal.

The NSA Acknowledged Receipt of EPIC's FOIA Request

19. The NSA transmitted a letter to EPIC dated July 1, 2009 ("NSA Letter 1").

20. NSA Letter 1 acknowledged the NSA's receipt of EPIC's FOIA Request and assigned it case number 58987.

21. NSA Letter 1 granted waiver of fees.

22. NSA Letter 1 denied expedited processing.

23. NSA Letter 1 did not make any substantive determination regarding EPIC's request.

EPIC Filed an Administrative Appeal with the NSA

24. On July 30, 2009, more than twenty working days after the NSA received EPIC's

FOIA Request, EPIC transmitted a written administrative appeal to the NSA (“EPIC’s Administrative Appeal 1”).

25. EPIC’s Administrative Appeal 1 was transmitted by certified mail to the NSA/CSS FOIA Appeal Authority at 9800 Savage Road Ste. 6248, Ft. George G. Meade, MD 20755-6248.

26. EPIC’s Administrative Appeal 1 appealed the NSA’s failure to make a timely determination regarding EPIC’s FOIA Request.

27. EPIC’s Administrative Appeal 1 also appealed the NSA’s denial of EPIC’s request for expedited processing.

The NSA Responded in Part to EPIC’s Administrative Appeal 1

28. The NSA/CSS FOIA Appeals Authority responded to EPIC in a letter dated August 12, 2009 (“NSA Letter 2”).

29. NSA Letter 2 granted EPIC’s appeal with respect to the request for expedited processing.

30. NSA Letter 2 did not make any substantive determination regarding EPIC’s FOIA request.

The NSA Responded in Part to EPIC’s FOIA Request

31. The NSA transmitted a letter to EPIC dated August 14, 2009 (“NSA Letter 3”).

32. NSA Letter 3 asserted that the agency had completed its search for responsive records.

33. NSA Letter 3 included two redacted documents which had been previously released under the FOIA (on 9/20/2006 and on 8/17/2007, respectively) and which the NSA identified as responsive to the third part of EPIC’s FOIA Request.

34. NSA Letter 3 included information regarding how to file an administrative appeal as to the redactions in the two included documents.

35. With respect to the first two parts of EPIC's FOIA Request, and with respect to other documents responsive to the third part, NSA Letter 3 stated only that since the request had been expedited, "the remaining material responsive has been assigned for review to determine releasability and will be completed as expeditiously as possible."

The NSA Made a Determination Regarding EPIC's FOIA Request

36. The NSA transmitted a letter to EPIC dated October 26, 2009 and signed by Pamela N. Phillips, Chief of the FOIA/PA Office ("NSA Letter 4").

37. NSA Letter 4 stated that EPIC's FOIA Request had been "further processed under the provisions of the FOIA."

38. NSA Letter 4 asserted that "no records responsive to item 2 of your request were located" and that "[t]hree documents (26 pages) responsive to items 1 and 3 of your request have been reviewed by this Agency as required by the FOIA."

39. NSA Letter 4 asserted that two documents responsive to item 3 of the request "have been withheld in their entirety" because they are "exempt from release pursuant to the fifth exemption of the FOIA" but gave no factual basis for this determination.

40. NSA Letter 4 also asserted that information in one document responsive to item 3 of the request is "currently and properly classified" and therefore exempt "pursuant to the first exemption of the FOIA" but gave no factual basis for this determination.

41. NSA Letter 4 also asserted that portions of both withheld documents are "exempt from disclosure pursuant to the third exemption of the FOIA which provides for the withholding of information specifically protected from disclosure by statute" and cited 18 U.S.C. § 798, 50

U.S.C. § 403-1(i), and 50 U.S.C. § 402 note, but gave no factual basis for this determination.

42. NSA Letter 4 stated that “the record responsive to item 1 of your request did not originate with this Agency” and that “the subject document has been referred to the National Security Council for review and direct response to you.”

EPIC Filed a Second Administrative Appeal with the NSA

43. On November 24, 2009, EPIC transmitted a written administrative appeal to the NSA (“EPIC’s Administrative Appeal 2”).

44. EPIC’s Administrative Appeal 2 was transmitted by certified mail to the NSA/CSS FOIA Appeal Authority at 9800 Savage Road Ste. 6248, Ft. George G. Meade, MD 20755-6248.

45. EPIC’s Administrative Appeal 2 appealed “the NSA’s failure to disclose the record identified as responsive to part 1 of EPIC’s FOIA Request.”

46. EPIC’s Administrative Appeal 2 also appealed “the NSA’s failure to disclose any records responsive to part 2 of EPIC’s FOIA request.”

47. EPIC’s Administrative Appeal 2 also appealed “the NSA’s failure to disclose the two records identified by the Agency in the October 26 letter as responsive to part 3 of EPIC’s FOIA request.”

The NSA Acknowledged Receipt of EPIC’s Administrative Appeal 2

48. The NSA/CSS FOIA Appeals Authority responded to EPIC in a letter dated December 18, 2009 (“NSA Letter 5”).

49. NSA Letter 5 acknowledged receipt of EPIC’s Administrative Appeal 2.

50. NSA Letter 5 stated that the Agency “will be unable to provide you a timely response,” and predicted “a decision on your appeal within the next nine months.”

The NSC Has Not Communicated to EPIC Regarding EPIC's FOIA Request

51. As of the date of this pleading, EPIC has not received any communication from the National Security Council regarding EPIC's FOIA Request.

Count I
(Against Defendant National Security Agency)
Violation of the FOIA: NSA's Failure to Comply with Statutory Deadlines

52. Paragraphs 1–51 above are hereby incorporated by reference as if set forth fully herein.

53. The NSA's failure to make a timely determination concerning EPIC's Administrative Appeal 2 violated the statutory deadlines imposed by the FOIA, including the deadlines set forth in 5 U.S.C. § 552(a)(6)(A) (2009).

54. EPIC has exhausted the applicable administrative remedies with respect to EPIC's FOIA Request, under the terms set forth in 5 U.S.C. § 552(a)(6)(C) (2009).

55. The NSA has wrongfully withheld responsive agency records from EPIC.

56. EPIC is entitled to injunctive relief compelling the release and disclosure of the requested agency records.

57. EPIC is further entitled to recover its attorneys' fees and costs in this action pursuant to 5 U.S.C. § 552(a)(4)(E).

Count II
(Against Defendant National Security Agency)
Violation of the FOIA: NSA's Failure to Disclose Responsive Agency Records

58. Paragraphs 1–57 above are hereby incorporated by reference as if set forth fully herein.

59. In responding to EPIC's FOIA Requests, the NSA violated the FOIA by failing to disclose agency records to EPIC that must be disclosed pursuant to the FOIA.

60. The NSA failed to disclose such agency records by, *inter alia*: 1) withholding responsive agency records pursuant to alleged exemptions although the alleged exemptions do not apply to the withheld records; and 2) withholding responsive agency records although nonexempt portions of the records are reasonably segregable from exempt portions.

61. In addition, the NSA failed to disclose an agency record in its possession and control by improperly referring a portion of EPIC's FOIA Request to the National Security Council.

62. EPIC is entitled to injunctive relief compelling the release and disclosure of the requested agency records.

63. EPIC is further entitled to recover its attorneys' fees and costs in this action pursuant to 5 U.S.C. § 552(a)(4)(E).

Count III
(Against Defendant National Security Council)
Violation of the FOIA: NSC's Failure to Disclose Responsive Agency Records

64. Paragraphs 1–63 above are hereby incorporated by reference as if set forth fully herein.

65. By referring EPIC's FOIA Request to defendant National Security Council, defendant National Security Agency represented that the NSC is subject to the FOIA with respect to this request.

66. The NSC has failed to disclose responsive agency records in its possession in response to the referral by the NSA.

67. EPIC is entitled to injunctive relief compelling the release and disclosure of the requested agency records.

68. EPIC is further entitled to recover its attorneys' fees and costs in this action

pursuant to 5 U.S.C. § 552(a)(4)(E).

Count IV
(Against Defendant National Security Agency)
Violation of the Administrative Procedure Act

69. Paragraphs 1–68 above are hereby incorporated by reference as if set forth fully herein.

70. By referring EPIC’s FOIA Request to defendant National Security Council, defendant National Security Agency violated the Administrative Procedure Act (“APA”), 5 U.S.C. § 706 (2009).

71. The NSA’s referral was arbitrary and capricious, an abuse of discretion, and otherwise not in accordance with the law.

72. The NSA’s referral exceeded the agency’s authority, because the FOIA (the ostensible statutory basis for the referral) does not permit the NSA to refer FOIA requests in this manner.

73. The NSA’s referral failed to observe procedures required by law, including, *inter alia*, the procedures set forth in 32 C.F.R. § 286.4.

Requested Relief

WHEREFORE, plaintiff prays that this Court:

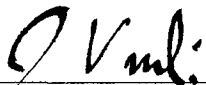
- A. order defendants to produce all responsive agency records within fourteen days of the Court’s Order in this matter;
- B. order defendant NSA to file, within fourteen days of the date of the Court’s Order in this matter, a “*Vaughn Index*,” *i.e.* an affidavit: 1) identifying each document withheld from disclosure; 2) stating defendant’s claimed statutory exemption as to each withheld document (or portion of a document); and 3) explaining why each withheld document is

exempt from disclosure;

- C. award plaintiff its costs and reasonable attorneys' fees incurred in this action pursuant to 5 U.S.C. § 552(a)(4)(E) (2009); and
- D. grant such other relief as the Court may deem just and proper.

Respectfully submitted,

By:



John Verdi, Esquire (DC Bar # 495764) ✓
Marc Rotenberg, Esquire (DC Bar # 422825)
Jared Kaprove, Esquire*
ELECTRONIC PRIVACY INFORMATION
CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Dated: February 4, 2010

*Mr. Kaprove is barred in the Commonwealth of Virginia.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY)	
INFORMATION CENTER)	
)	Case No. 1:10-cv-00196-RMU
Plaintiff,)	
)	
v.)	
)	
NATIONAL SECURITY AGENCY;)	
NATIONAL SECURITY COUNCIL)	
)	
Defendants.)	

ANSWER

Defendant National Security Agency (“Defendant” or “NSA”), by and through its undersigned counsel, answers Plaintiff’s Complaint (“Complaint”) as follows. To the extent that any unnumbered headings in the Complaint are deemed to contain allegations, Defendant denies those allegations:

1. The allegations contained in paragraph 1 of the Complaint set forth Plaintiff’s characterization of the action to which no response is required. To the extent that a response is deemed necessary, these allegations are denied.
2. The allegations contained in paragraph 2 of the Complaint set forth conclusions of law to which no response is required.
3. Defendant is without sufficient knowledge or information to form a belief as to the truth of the allegations contained in paragraph 3 of the Complaint, and, on that basis, denies the allegations.
4. Defendant denies the allegations contained within the first sentence of paragraph

4 of the Complaint, except admits that the NSA is an element of the Intelligence Community, that the NSA is a Defense agency, and that the Secretary of Defense exercises authority, direction, and control over the NSA. The allegations contained in the second sentence of paragraph 4 of the Complaint set forth conclusions of law to which no response is required.

5. The allegations contained in paragraph 5 of the Complaint set forth conclusions of law to which no response is required.
6. Defendant admits the allegations contained in paragraph 6 of the Complaint.
7. Defendant denies the allegations contained in paragraph 7 of the Complaint, except that Defendant admits that the full text of National Security Presidential Directive 54 has not been publicly released.
8. Defendant admits the allegations contained in paragraph 8 of the Complaint.
9. Defendant is without sufficient knowledge or information to form a belief as to the truth of the allegations contained paragraph 9 of the Complaint, and, on that basis, denies the allegations.
10. The allegations contained in paragraph 10 of the Complaint set forth Plaintiff's characterization of the cited letter, and thus no response is required. Defendant respectfully refers the Court to the cited letter for the full and accurate statement of its contents.
11. Defendant is without sufficient knowledge or information to form a belief as to the truth of the allegations contained paragraph 11 of the Complaint, and, on that basis, denies the allegations.
12. The allegations contained in paragraph 12 of the Complaint set forth Plaintiff's characterization of the cited letter, and thus no response is required. Defendant respectfully refers the Court to the cited letter for the full and accurate statement

of its contents.

13. Defendant admits the allegations contained in paragraph 13 of the Complaint.
14. Defendant admits the allegations contained in paragraph 14 of the Complaint.
15. Defendant admits the allegations contained in paragraph 15 of the Complaint.
16. The allegations contained in paragraph 16 of the Complaint set forth Plaintiff's characterization of the cited FOIA request, and thus no response is required. Defendant respectfully refers the Court to the cited FOIA request for the full and accurate statement of its contents.
17. The allegations contained in paragraph 17 of the Complaint set forth Plaintiff's characterization of the cited FOIA request, and thus no response is required. Defendant respectfully refers the Court to the cited FOIA request for the full and accurate statement of its contents.
18. Defendant is without sufficient knowledge or information to form a belief as to the truth of the allegations contained paragraph 18 of the Complaint, and, on that basis, denies the allegations.
19. Defendant admits the allegations contained in paragraph 19 of the Complaint.
20. Defendant admits the allegations contained in paragraph 20 of the Complaint.
21. The allegations contained in paragraph 21 of the Complaint set forth Plaintiff's characterization of the cited July 1, 2009 letter, and thus no response is required. Defendant respectfully refers the Court to the cited letter for the full and accurate statement of its contents.
22. The allegations contained in paragraph 22 of the Complaint set forth Plaintiff's characterization of the cited July 1, 2009 letter, and thus no response is required. Defendant respectfully refers the Court to the cited letter for the full and accurate statement of its contents.

23. The allegations contained in paragraph 23 of the Complaint set forth Plaintiff's characterization of the cited July 1, 2009 letter, and thus no response is required. Defendant respectfully refers the Court to the cited letter for the full and accurate statement of its contents.
24. The allegations contained in paragraph 24 of the Complaint set forth Plaintiff's characterization of the cited July 30, 2009 letter, and thus no response is required. Defendant respectfully refers the Court to the cited letter for the full and accurate statement of its contents.
25. Defendant admits the allegations contained in paragraph 25 of the Complaint.
26. The allegations contained in paragraph 26 of the Complaint set forth Plaintiff's characterization of the cited July 30, 2009 letter, and thus no response is required. Defendant respectfully refers the Court to the cited letter for the full and accurate statement of its contents.
27. The allegations contained in paragraph 27 of the Complaint set forth Plaintiff's characterization of the cited July 30, 2009 letter, and thus no response is required. Defendant respectfully refers the Court to the cited letter for the full and accurate statement of its contents.
28. Defendant admits the allegations contained in paragraph 28 of the Complaint.
29. The allegations contained in paragraph 29 of the Complaint set forth Plaintiff's characterization of the cited August 12, 2009 letter, and thus no response is required. Defendant admits that the August 12, 2009 letter granted Plaintiff's request for expedited processing. Defendant respectfully refers the Court to the cited letter for the full and accurate statement of its contents.
30. The allegations contained in paragraph 30 of the Complaint set forth Plaintiff's characterization of the cited August 12, 2009 letter, and thus no response is

required. Defendant respectfully refers the Court to the cited letter for the full and accurate statement of its contents.

31. Defendant admits the allegations contained in paragraph 31 of the Complaint.

32–35 The allegations contained in paragraphs 32–35 of the Complaint set forth Plaintiff’s characterization of the cited August 14, 2009 letter, and thus no response is required. Defendant respectfully refers the Court to the cited letter for the full and accurate statement of its contents.

36. Defendant admits the allegations contained in paragraph 36 of the Complaint.

37–42 The allegations contained in paragraphs 37–42 of the Complaint set forth Plaintiff’s characterization of the cited October 26, 2009 letter, and thus no response is required. Defendant respectfully refers the Court to the cited letter for the full and accurate statement of its contents.

43. Defendant admits the allegations contained in paragraph 43 of the Complaint.

44. Defendant admits the allegations contained in paragraph 44 of the Complaint.

45–47 The allegations contained in paragraphs 45–47 of the Complaint set forth Plaintiff’s characterization of the cited November 24, 2009 letter, not allegations of fact, and thus no response is required. Defendant respectfully refers the Court to the cited letter for the full and accurate statement of its contents.

48. Defendant denies the allegations contained in paragraph 48 of the Complaint, except admits that the NSA Associate General Counsel for Litigation responded to Plaintiff in a letter dated December 18, 2009.

49. Defendant admits the allegations contained in paragraph 49 of the Complaint.

50. The allegations contained in paragraph 50 of the Complaint set forth Plaintiff’s characterization of the cited December 18, 2009 letter, and thus no response is required. Defendant respectfully refers the Court to the cited letter for the full

and accurate statement of its contents.

51. Defendant is without sufficient knowledge or information to form a belief as to the truth of the allegations contained in paragraph 51 of the Complaint, and, on that basis, denies the allegations.

52. In response to the recital contained in paragraph 52 of the Complaint, Defendant incorporates by reference the responses to paragraphs 1 through 51 of the Complaint as if fully set forth herein.

53–57 The allegations contained in paragraphs 53–57 of the Complaint set forth conclusions of law to which no response is required. To the extent that a response is deemed necessary, these allegations are denied. Defendant respectfully refers the Court to the cited statutory provision for the full and accurate statement of its contents.

58. In response to the recital contained in paragraph 58 of the Complaint, Defendant incorporates by reference the responses to paragraphs 1 through 57 of the Complaint as if fully set forth herein.

59–63 The allegations contained in paragraphs 59–63 of the Complaint set forth conclusions of law to which no response is required. To the extent that a response is deemed necessary, these allegations are denied.

64. In response to the recital contained in paragraph 64 of the Complaint, Defendant incorporates by reference the responses to paragraphs 1 through 63 of the Complaint as if fully set forth herein.

65–68 Defendant avers that no response is required to the allegations contained in paragraphs 65–68 of the Complaint because they are directed only to Defendant National Security Council.

69. In response to the recital contained in paragraph 69 of the Complaint, Defendant

incorporates by reference the responses to paragraphs 1 through 68 of the Complaint as if fully set forth herein.

70–73 Defendant avers that no response is required to the allegations contained in paragraphs 70–73 of the Complaint because these allegations are addressed by the pending Partial Motion to Dismiss filed by Defendant.

The remainder of the Complaint sets forth Plaintiff’s request for relief, to which no response is required. To the extent that a response is required, Defendant denies that Plaintiff is entitled to any relief. Any allegation not expressly answered is hereby denied.

FIRST DEFENSE

The allegations of the Complaint fail to state a claim on which relief may be granted.

SECOND DEFENSE

Plaintiff is not entitled to compel the production of records protected from disclosure by one or more exemptions to the Freedom of Information Act (“FOIA”), 5 U.S.C. § 552.

DATED: March 25, 2010

Respectfully Submitted,

TONY WEST
Assistant Attorney General

RONALD C. MACHEN
United States Attorney

ELIZABETH J. SHAPIRO
Deputy Director

/s/ Joshua Wilkenfeld
JOSHUA WILKENFELD
Trial Attorney

United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W.
Washington, D.C. 20530
Tel: (202) 305-7920
Fax: (202) 616-8470
Email: joshua.i.wilkenfeld@usdoj.gov

Counsel for Defendant

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that a copy of the foregoing filing has been furnished via CM/ECF to counsel for Plaintiff, John Verdi, Esq., of the Electronic Privacy Information Center, on this 25th day of March, 2010.

/s/ Joshua Wilkenfeld

Joshua Wilkenfeld

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

ELECTRONIC PRIVACY INFORMATION
CENTER,

Plaintiff,

v.

NATIONAL SECURITY AGENCY, *et al.*

Defendants.

Civil Action No. 10-0196 (BAH)

MEMORANDUM OPINION

Pending before the Court is the partial motion to dismiss by the National Security Agency (“NSA”) and the National Security Council (“NSC”) two of the four claims in the Complaint. These claims stem from a Freedom of Information Act (“FOIA”) request that the plaintiff, Electronic Privacy Information Center (“EPIC”), filed with the NSA seeking information related to the Comprehensive National Cybersecurity Initiative, a multi-agency federal initiative to ensure the security of the nation’s online infrastructure. In this case, the NSA referred part of the plaintiff’s FOIA request to the NSC since a responsive document in the NSA’s possession had originated with the NSC. The plaintiff brought this lawsuit against both the NSA and NSC to compel the production of documents responsive to its FOIA request. The plaintiff believes that releasing the documents it seeks “would provide the opportunity for meaningful public participation in the development of new security measures that may have a significant impact on civil liberties, such as privacy.” Def.’s Partial Mot. to Dismiss (“Defs.’ Mot.”), Ex. A at 2-3 (Plaintiff’s FOIA Appeal). The defendants now seek to dismiss the plaintiff’s claims in Count III, which alleges that the NSC “failed to disclose responsive agency records in its possession in response to the referral by the NSA,” Compl. ¶ 66, and in Count IV, which alleges that the NSA

violated the Administrative Procedure Act when it referred the FOIA request to the NSC. *Id.* ¶ 72. For the reasons discussed below, the Court will grant the partial motion to dismiss.¹

I. BACKGROUND

On June 25, 2009, Plaintiff EPIC submitted a FOIA request to the NSA seeking documents related to the Comprehensive National Cybersecurity Initiative (“CNCI”), an initiative established by former President George W. Bush that outlines federal cyber-security goals. *Id.* ¶¶ 6, 10, 15.

The plaintiff is a not-for-profit public interest research organization that reviews federal activities and policies to determine their possible impact on civil liberties and privacy interests. *Id.* ¶ 3. The NSA is an agency within the Department of Defense that is responsible for shielding our nation’s coded communications from interception by foreign governments and for secretly intercepting intelligence communications from foreign nations. *See Founding Church of Scientology of Wash., D.C., Inc. v. NSA*, 610 F.2d 824, 825 (D.C. Cir. 1979); *Larson v. Dep’t of State*, No. 02-01937, 2005 WL 3276303, at *17 (D.D.C. Aug. 10, 2005), *aff’d*, 565 F.3d 857 (D.C. Cir. 2009).

President Bush established the CNCI on January 8, 2008 by issuing National Security Presidential Directive 54 (“NSPD 54”), also known as Homeland Security Presidential Directive 23. *Id.* ¶¶ 6, 8. The contents of NSPD 54 have not been released to the public. *Id.* ¶ 7. The CNCI, as described by the Senate Committee on Homeland Security and Governmental Affairs,

¹ The Court has jurisdiction over this case pursuant to 28 U.S.C. § 1331 because this case arises under a federal law – the Freedom of Information Act – and “the district courts . . . have original jurisdiction of all civil actions arising under the Constitution, laws, or treaties of the United States.” 28 U.S.C. § 1331. Jurisdiction is also established by the FOIA statute itself, which provides that “[o]n complaint, the district court of the United States. . . in the District of Columbia, has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant.” 5 U.S.C. § 552(a)(4)(B). Section 552(a)(4)(B) also makes venue proper in this District. *See In re Scott*, 709 F.2d 717, 720 (D.C. Cir. 1983) (citing 5 U.S.C. § 552(a)(4)(B) for the proposition that Congress expressly intended “to render the District of Columbia an all-purpose forum in FOIA cases.”).

is a “multi-agency, multi-year plan that lays out twelve steps to securing the federal government’s cyber networks.” *Id.* ¶¶ 9-10. The CNCI was formed “to improve how the federal government protects sensitive information from hackers and nation states trying to break into agency networks.” Defs.’ Mot., Ex. A at 1-2.

On June 25, 2009, the plaintiff submitted a written FOIA request to the NSA that, in its entirety, sought the following documents:

- a. The text of the National Security Presidential Directive 54 otherwise referred to as Homeland Security Presidential Directive 23;
- b. The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation; and
- c. Any privacy policies related to either the Directive, the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative.

Compl. ¶ 15. The plaintiff also requested an expedited response to its request. *Id.* ¶ 16. The expedited processing request was initially denied on July 1, 2009, but was granted on August 12, 2009, after the plaintiff filed an administrative appeal. *Id.* ¶¶ 22, 29.

The NSA responded to the plaintiff’s request on August 14, 2009 and produced two redacted documents that had been previously released under FOIA, although the Complaint does not indicate whether the plaintiff was the previous recipient of the documents. *Id.* ¶ 33. On October 26, 2009, the NSA informed the plaintiff that its request had been processed further and that three records responsive to the request had been located. *Id.* ¶¶ 36-38. The NSA withheld two of the three records in their entirety, claiming that these two records were exempt from release pursuant to various statutory exemptions to FOIA’s disclosure requirements. *Id.* ¶¶ 39-41. The plaintiff’s Complaint indicates the NSA did not provide a factual basis for its determinations that the claimed FOIA exemptions were applicable to the withheld documents.

Id. As for the third record responsive to the plaintiff's request, the NSA indicated that this record did not originate with the NSA, but rather with the NSC, and that the record had therefore been referred to the NSC for "review and direct response to [EPIC]." *Id.* ¶ 42. The NSC is a presidential advisory group composed of the President, Vice-President, Secretary of State, Secretary of Defense, and other cabinet-level officials, including the National Security Advisor, that advises the President of the United States on national security and foreign policy issues. *Armstrong v. Exec. Office of the President*, 90 F.3d 553, 556 (D.C. Cir. 1996); 50 U.S.C. § 402(a).

The plaintiff filed a written administrative appeal to the NSA on November 24, 2009, contesting the NSA's failure to disclose the records that were found responsive to the FOIA request. *Id.* ¶¶ 43-47. The NSA acknowledged receipt of the appeal on December 18, 2009 and predicted a decision on the plaintiff's appeal "within the next nine months." *Id.* ¶¶ 48-50. As of February 4, 2010, the date this case was filed, the plaintiff had not received any communication from the NSC regarding the FOIA request. *Id.* ¶ 51.

The plaintiff brought this case to compel the defendants NSA and NSC to produce "all responsive agency records" and to order the NSA to file a *Vaughn* index that identifies each withheld document, states the NSA's claimed statutory exemption as to each withheld document, and explains why each withheld document is exempt from disclosure. Compl., Requested Relief, ¶¶ A-B. In Count I of the Complaint, the plaintiff alleges that the NSA violated FOIA by failing to comply with statutory deadlines regarding its administrative appeal. *Id.* ¶¶ 52-57. In Count II, the plaintiff alleges that the NSA failed to disclose responsive agency records through (1) withholding records that are not exempt, (2) withholding nonexempt portions of records that are reasonably segregable from exempt portions, and (3) improperly referring a portion of the

plaintiff's FOIA request to the NSC. *Id.* ¶¶ 58-63. In Count III, which is directed against the NSC, the plaintiff alleges that the NSC violated FOIA by failing to disclose responsive agency records in its possession in response to the referral by the NSA. *Id.* ¶¶ 64-68. Lastly, in Count IV, the plaintiff alleges that the NSA's referral of the FOIA request to the NSC violated the Administrative Procedure Act ("APA"), 5 U.S.C. § 500 *et seq.* *Id.* ¶ 70.

On March 25, 2010, the defendants filed a partial motion to dismiss Counts III and IV pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure. Defs.' Mot. at 1.² The defendants argue that since the NSC is not an entity subject to FOIA's disclosure requirements, the Court should dismiss the plaintiff's claims against the NSC (i.e., Count III). Mem. in Supp. of Defs.' Partial Mot. to Dismiss ("Defs.' Mem.") at 1-2. The defendants further argue that the Court should dismiss Count IV, the plaintiff's APA claim against the NSA, because FOIA provides an adequate alternative remedy for the relief sought in the plaintiff's APA claim. *Id.* at 2. The defendants' partial motion to dismiss is presently before the Court.³

II. DISCUSSION

A. Standard of Review

Congress enacted FOIA to promote transparency across the government. See 5 U.S.C. § 552; *Quick v. U.S. Dep't of Commerce, Nat'l Inst. of Standards & Tech.*, No. 09-02064, 2011 WL 1326928, at *3 (D.D.C. April 7, 2011) (citing *Stern v. FBI*, 737 F.2d 84, 88 (D.C. Cir. 1984)). The Supreme Court has explained that FOIA is "a means for citizens to know 'what their Government is up to.' This phrase should not be dismissed as a convenient formalism. It defines a structural necessity in a real democracy." *Nat'l Archives & Records Admin. v. Favish*,

² This case was reassigned to the presiding judge on January 20, 2011.

³ Since the present motion to dismiss addresses only Counts III and IV of the Complaint, the Court does not reach the merits of Counts I and II; namely, whether the NSA has validly asserted certain FOIA exemptions and fulfilled its statutory disclosure obligations.

541 U.S. 157, 171-172 (2004) (internal citations omitted). “The basic purpose of FOIA 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.” *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978). The strong interest in transparency must be tempered, however, by the “legitimate governmental and private interests [that] could be harmed by release of certain types of information.” *United Techs. Corp. v. U.S. Dep’t of Defense*, 601 F.3d 557, 559 (D.C. Cir. 2010); *see also Critical Mass Energy Project v. Nuclear Regulatory Comm’n*, 975 F.2d 871, 872 (D.C. Cir. 1992). Accordingly, Congress included nine exemptions permitting agencies to withhold information from FOIA disclosure. 5 U.S.C. § 552(b). “These exemptions are explicitly made exclusive, and must be narrowly construed.” *Milner v. Dep’t of the Navy*, 131 S. Ct. 1259, 1262 (2011) (internal quotations and citations omitted) (citing *FBI v. Abramson*, 456 U.S. 615, 630 (1982)); *see also Pub. Citizen, Inc. v. Office of Management and Budget*, 598 F.3d 865, 869 (D.C. Cir. 2010).

To survive a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), a plaintiff need only plead “enough facts to state a claim to relief that is plausible on its face” and to “nudge [] [his or her] claims across the line from conceivable to plausible.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007); Fed. R. Civ. P. 12(b)(6). “[A] complaint [does not] suffice if it tenders naked assertions devoid of further factual enhancement.” *Ashcroft v. Iqbal*, 129 S.Ct. 1937, 1949 (2009) (internal quotation marks omitted) (citing *Twombly*, 550 U.S. at 557). Instead, the complaint must plead facts that are more than “merely consistent with” a defendant’s liability; “the plaintiff [must plead] factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Id.* at 1949, 1940.

The Court must “assume all the allegations in the complaint are true (even if doubtful in fact) ... [and] must give the plaintiff the benefit of all reasonable inferences derived from the facts alleged.” *Aktieselskabet AF 21. November 2001 v. Fame Jeans Inc.*, 525 F.3d 8, 17 (D.C. Cir. 2008) (internal quotations and citations omitted). When the Court reviews legal conclusions, however, “the tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable.” *In re Interbank Funding Corp. Sec. Litig.*, 629 F.3d 213, 218 (D.C. Cir. 2010) (quoting *Iqbal*, 129 S.Ct. at 1949).

B. Analysis

1. The NSC is not an Agency Subject to FOIA

The text of FOIA makes clear that the statute applies to “agenc[ies]” only. *See* 5 U.S.C. § 552(a) (“Each agency shall make available to the public information as follows...”). The statutory definition of an “agency” explicitly includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President). *See* 5 U.S.C. § 552(f). Using legislative history as its guide, however, the Supreme Court has held that “the President’s immediate personal staff or units in the Executive Office whose sole function is to advise and assist the President are not included within the term ‘agency’ under the FOIA.” *Kissinger v. Reporters Comm. for Freedom of the Press*, 445 U.S. 136, 155 (1980) (quoting H.R. Rep. No. 93-1380, at 15 (1974) (Conf. Rep.)) (internal quotations and citations omitted).

The National Security Act of 1947 established the NSC to “advise the President with respect to the integration of domestic, foreign, and military policies relating to national security.” 50 U.S.C. § 402(a); *Armstrong*, 90 F.3d at 556. Pursuant to the Reorganization Plan No. 4 of

1949, the NSC was transferred to the Executive Office of the President. Reorg. Plan No. 4 of 1949, 14 Fed. Reg. 5227, 63 Stat. 1067 (1949).

This Circuit has unambiguously held that the NSC is not an agency subject to FOIA. *Armstrong*, 90 F.3d at 565 (“[W]e hold that . . . the NSC is not an agency subject to the FOIA.”); *see also Citizens for Responsibility and Ethics in Wash. v. Office of Admin.*, 566 F.3d 219, 223 (D.C. Cir. 2009) (“Nor is the National Security Council . . . covered by FOIA because it plays no ‘substantive role apart from that of the President, as opposed to a coordinating role on behalf of the President.’”) (quoting *Armstrong*, 90 F.3d at 565); *Alexander v. FBI*, 691 F. Supp. 2d 182, 189 (D.D.C. 2010) (“[T]he National Security Council [and certain other Executive offices] have all been excluded from FOIA’s definition of agency because they are either part of the President’s immediate staff or have the sole function of advising and assisting the President.”). In ruling that the NSC is not an agency subject to FOIA, the D.C. Circuit in *Armstrong* applied a three-factor test to determine whether an entity is an agency subject to FOIA. *See Armstrong*, 90 F.3d at 558-65 (applying three-factor test described in *Meyer v. Bush*, 981 F.2d 1288, 1293 (D.C. Cir. 1993)). The test requires the court to inquire into (1) “how close operationally the group is to the President,” (2) “whether it has a self-contained structure,” and (3) “the nature of its delegat[ed]” authority. *Id.* These three factors do not need to be weighed equally; rather, each factor warrants consideration insofar as it is illuminating in the particular case. *Armstrong*, 90 F.3d at 558. The court found that the NSC has a firm structure, making it similar to an agency, but ultimately concluded that because the NSC operates in such close proximity to the President – who chairs it – and does not exercise substantial independent authority, it is “more like the President’s immediate personal staff.” *Id.* at 567. Accordingly, the D.C. Circuit held that the

“NSC is not an agency within the meaning of the FOIA.” *Id* at 556. That conclusion is binding upon this Court.

Organizations that are not an “agency” under FOIA are neither required to respond to a FOIA request nor subject to a FOIA lawsuit. *See Citizens for Responsibility and Ethics in Wash.*, 566 F.3d at 225; *Sweetland v. Walters*, 60 F.3d 852, 855 (D.C. Cir. 1995). Since the D.C. Circuit squarely held in *Armstrong* that the NSC is not an agency subject to FOIA, the NSC cannot be compelled to respond to a FOIA request.

The plaintiff attempts to distinguish *Armstrong* because the FOIA request in that case was made directly to the NSC, while, in this case, the NSA referred the request to the NSC. *See* Pl.’s Opp’n to Defs.’ Partial Mot. to Dismiss (“Pl.’s Opp’n”) at 3. The plaintiff contends that, by referring the FOIA request to the NSC, the NSA “treat[ed] the NSC as if it were an agency subject to the FOIA,” and therefore this Court should find the NSC subject to FOIA in this case. *Id* at 4.

The plaintiff’s argument is unpersuasive. It is true that agencies that receive FOIA requests and discover responsive documents that were created by another agency may forward, or “refer,” those requests to the agency that “originated” the document. *See Schoenman v. FBI*, No. 04-2202, 2009 WL 763065, at *6 (D.D.C. Mar. 19, 2009) (“A ‘referral’ occurs when, in the course of reviewing documents responsive to a FOIA [] request, an agency finds a document that was originated by a second agency. When that occurs, the agency receiving the FOIA [] request forwards, or ‘refers,’ the document(s) at issue to the second agency, which then becomes responsible for directly responding to the requester as to those documents.”) (internal citations omitted). Here, however, the question is whether an entity *that is not an agency subject to FOIA* must respond to a FOIA request referred from an agency that is subject to FOIA. This question

appears to be one of first impression in this Circuit, since neither the parties nor the Court have located authority that directly addresses the issue. The Court finds the answer to this question to be clear-cut: The answer is no. An entity that is not subject to FOIA cannot unilaterally be made subject to the statute by any action of an agency, including referral of a FOIA request. It would defy logic and well-settled legal norms if an agency could unilaterally expand the scope of FOIA by referring requests to entities beyond FOIA's ambit.

The plaintiff points out, correctly, that the NSA's internal regulations permit it to refer FOIA requests for records originated "by other agencies" to "the originating agency's FOIA Authority." 32 C.F.R. § 299.5(k). Yet, by referring the plaintiff's FOIA request to the NSC – which is not an "agency" for FOIA purposes – the NSA does not thereby transform the NSC into an agency and render the NSC "subject to the FOIA with respect to this request," as the plaintiff alleges. Compl. ¶ 65. As an agency within the Executive Branch, the NSA does not have the power to expand FOIA's reach beyond the scope intended by Congress. *See Emily's List v. FEC*, 581 F.3d 1, 26 (D.C. Cir. 2009) ("The Executive Branch cannot make law, but instead executes laws enacted by the Legislative Branch."). "[A]n agency literally has no power to act . . . unless and until Congress confers power upon it." *La. Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986). As the Supreme Court has explained, "[a]n agency may not confer power upon itself. To permit an agency to expand its power in the face of a congressional limitation on its jurisdiction would be to grant to the agency power to override Congress. This we are both unwilling and unable to do." *Id.* at 374-75; *see also Cal. Indep. Sys. Operator Corp. v. FERC*, 372 F.3d 395, 398 (D.C. Cir. 2004). Even assuming, *arguendo*, that the NSA's regulations authorized a referral to the NSC, the NSA's regulations cannot trump Congressional intent to

exclude close presidential advisors from FOIA. *See Kissinger*, 455 U.S. at 156; *see also Armstrong*, 90 F.3d at 558.

The plaintiff further argues that even if the NSC is not technically an “agency” subject to the FOIA, the NSA should be held to its representation “that the NSC would ‘review’ the request and provide a ‘direct response.’” Pl.’s Opp’n at 4. Indeed, the plaintiff contends reliance on this representation was reasonable since, before the D.C. Circuit decided in *Armstrong* that the NSC was not subject to FOIA, the NSC had voluntarily responded to certain FOIA requests while asserting that it was not statutorily required to do so. *See* Pl.’s Opp’n at 4-5 (citing *Armstrong*, 90 F.3d at 557, 566). This argument essentially rests on an equitable estoppel theory, but equitable estoppel is not available against the federal government, except where the plaintiff has relied on the government’s conduct “in such a manner as to change [its] position for the worse,” and where the government has engaged in “affirmative misconduct.” *Morris Commc’ns, Inc. v. FCC*, 566 F.3d 184, 191 (D.C. Cir. 2009). Such circumstances are absent from this case. *See, e.g., id.* at 192 (finding an agency’s “three-year silence” in response to a request for waiver of automatic cancellation of radio licenses was “egregious” but did not constitute “affirmative misconduct”). Moreover, the D.C. Circuit expressly addressed the issue of the NSC’s prior voluntary disclosures in *Armstrong*: “That the NSC . . . voluntarily subjected certain of its records to the FOIA and the [Federal Records Act] does not reflect any intention to concede, and should not be taken to establish as a matter of law, that the NSC is subject to those statutes.” *Armstrong*, 90 F.3d at 566. In short, the law in this Circuit since *Armstrong* is that the NSC is not subject to FOIA requests.

Lastly, the plaintiff asks this Court to find the NSC subject to FOIA in this case in order to avoid its FOIA request from being “toss[ed]... down a procedural black hole, with neither [the

NSA nor the NSC being] required to disclose an agency record that they both possess.” Pl.’s Opp’n at 3. The plaintiff contends that the defendant’s arguments would trap its request in a Catch-22 based on two “clearly contradictory” premises: (1) the NSA properly referred EPIC’s FOIA request to the NSC; and (2) the NSC need not respond to the request because it is not subject to FOIA. *Id.* Dismissing the plaintiff’s claim against the NSC, however, does not leave the plaintiff’s request stuck in limbo, as the plaintiff fears, because the plaintiff can still pursue its claim against the NSA for wrongfully withholding an agency record in its possession.

Indeed, Count II of the Complaint alleges that the NSA violated FOIA by “improperly referring a portion of EPIC’s FOIA request to the [NSC].” Compl. ¶ 61. The defendants have not moved to dismiss this count and the defendants concede that the plaintiff can continue its prosecution of this claim against the NSA.⁴ *See* Defs.’ Reply Mem. at 4. While the NSC is not subject to FOIA requests, the NSA’s referral of the FOIA request to the NSC does not relieve the NSA of its continuing obligation to respond to the request. An agency may only properly refer a FOIA request to another agency when doing so does not constitute an improper withholding of agency records. *See* 5 U.S.C. § 552(a)(4)(B); *Campaign for Responsible Transplantation v. FDA*, 511 F.3d 187, 190 (D.C. Cir. 2007) (“Under 5 U.S.C. § 552(a)(4)(B), when responsive documents have been unjustifiably withheld, a district court has the power to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld.”) (internal quotation omitted). A referral of a FOIA request could be considered a “withholding” if “its net effect is to impair the requester’s ability to obtain the records or

⁴ The NSA may intend to argue that its referral of the plaintiff’s request to the NSC was a proper inter-agency referral that relieved the NSA of any obligation to respond to the request. The plaintiff has inferred as much from its interpretation of a footnote in the defendants’ memorandum, *see* Pl.’s Opp’n at 5 (citing Defs.’ Mem. at 5 n.4), but the Court notes that the NSA has not directly advanced this position before the Court. The Court agrees with the plaintiff that such a position would be facially inconsistent with the defendants’ arguments regarding the instant motion.

significantly to increase the amount of time he must wait to obtain them.” *McGehee v. CIA*, 697 F.2d 1095, 1110 (D.C. Cir. 1983), *vacated in part and aff’d in part*, 711 F.2d 1076 (D.C. Cir. 1983). Such a withholding would be “improper” when it fails to satisfy a reasonableness standard for evaluating agency FOIA procedures. *Id.* at 1110. In considering the plaintiff’s claims against the NSA, which the defendants have not moved to dismiss, this Court will have an opportunity to evaluate the propriety of the NSA’s handling of all documents responsive to the FOIA request, including the document that originated with the NSC.

The NSA’s referral of the plaintiff’s FOIA claim to the NSC, even combined with its representation that the NSC would respond directly to the plaintiff’s request, does not subject the NSC to FOIA. Accordingly, the Court will grant the defendants’ motion to dismiss Count III of the plaintiff’s Complaint and dismiss the NSC from this action.

2. The FOIA Provides the Plaintiff with an Adequate Alternative Remedy to the Plaintiff’s APA Claim

Count IV of the plaintiff’s Complaint alleges that the NSA violated the APA by referring the FOIA request to the NSC. Compl. ¶ 70; *cf.* 5 U.S.C. § 706(2)(A). Specifically, the plaintiff claims the referral was “arbitrary, capricious, an abuse of discretion, and otherwise not in accordance with the law” because the FOIA does not permit the NSA to refer FOIA requests in this manner and because the NSA’s referral failed to observe procedures required by law, including the procedures set forth in NSA regulations codified at 32 C.F.R. § 286.4.⁵ Compl. ¶¶

⁵ The plaintiff does not make clear the specific sub-part of 32 C.F.R. § 286.4 that the NSA allegedly violated. *See* Compl. ¶ 73. The plaintiff may be relying on § 286.4(i)(7), which governs how Department of Defense (“DoD”) Components, such as the NSA, respond to requests involving NSC records. According to § 286.4(i)(7), “DoD records in which the NSC or White House has a concurrent reviewing interest, and NSC, White House, or [White House Military Office] records discovered in DoD Components’ files shall be forwarded to the Directorate for Freedom of Information and Security Review (DFOISR). The DFOISR shall coordinate with the NSC, White House, or WHMO and return the records to the originating agency after coordination.”

71-73. The defendant has moved to dismiss the plaintiff's APA claim because an adequate remedy is available under FOIA. *See* Defs.' Mem. at 7.

The APA permits judicial review of "final agency action[s] for which there is no other adequate remedy in a court." *See* 5 U.S.C. § 704. The Supreme Court has held that the APA's judicial review provision "does not provide additional judicial remedies in situations where the Congress has provided special and adequate review procedures." *Bowen v. Mass.*, 487 U.S. 879, 903 (1988). In this Circuit, the alternative remedy "need not provide relief identical to relief under the APA, so long as it offers relief of the same genre." *Garcia v. Vilsack*, 563 F.3d 519, 522 (D.C. Cir. 2009). "[W]here a statute affords an opportunity for *de novo* district-court review" of the agency action, APA review is precluded since "Congress did not intend to permit a litigant challenging an administrative denial . . . to utilize simultaneously both [the statute's review provision] and the APA." *El Rio Santa Cruz Neighborhood Health Ctr., Inc. v. U.S. Dep't of Health and Human Servs.*, 396 F.3d 1265, 1270 (D.C. Cir. 2005).

APA claims arising out of an agency's response to a FOIA request must be dismissed when they seek relief that can be obtained through a FOIA claim itself. *See* *Feinman v. FBI*, 713 F. Supp. 2d 70, 76 (D.D.C. 2010) ("This Court and others have uniformly declined jurisdiction over APA claims that sought remedies made available by FOIA."); *Kenney v. U.S. Dep't of Justice*, 603 F. Supp. 2d 184, 190 (D.D.C. 2009) ("Plaintiff's claim that the [agency] improperly withheld agency records that were responsive to his FOIA request is, of course, reviewable under the FOIA itself. . . Accordingly, plaintiff does not also have access to judicial review under the APA.") (internal citations omitted); *People for the American Way Found. v. Nat'l Parks Serv.*, 503 F. Supp. 2d 284, 308 (D.D.C. 2007) (finding agency's alleged failure to disclose documents responsive to plaintiff's FOIA request not reviewable under APA); *Edmonds Institute v. U.S.*

Dep't of Interior, 383 F. Supp. 2d 105, 111 (D.D.C. 2005) (finding FOIA provided adequate remedy and dismissing plaintiff's claim under the APA that the agency failed to respond to FOIA requests within statutory timeline).

The plaintiff asserts that “[c]ourts often adjudicate lawsuits involving related APA claims and FOIA claims,” citing in support of this proposition *Snyder v. CIA*, 230 F. Supp. 2d 17 (D.D.C. 2002). Pl.’s Opp’n at 8. In that case, a court in this District appeared to have addressed an APA claim challenging the defendant agency’s FOIA referral procedures. A close reading of the case reveals, however, that the statutory provision that the court actually applied in adjudicating the “APA” claim in *Snyder* was “Section 552(a)(4)(B) of the Administrative Procedures Act” or “5 U.S.C. § 552(a)(4)(B)” – i.e., the judicial review provisions of the FOIA statute, not the general APA judicial review provisions, which are codified at 5 U.S.C §§ 704-706. Thus, *Snyder* does not actually present a situation in which a court in this District entertained a FOIA claim and a related APA claim under 5 U.S.C. § 706, as the plaintiff contends.⁶ Even if *Snyder* did present such a situation, however, the Court would still dismiss the APA claim in this case in view of the binding precedents from the D.C. Circuit.⁷

The plaintiff asserts that the cases in which APA claims have been dismissed from FOIA suits are distinguishable from the instant situation, since the plaintiff here is asserting an APA violation that stems not from failure to disclose documents responsive to its FOIA request,

⁶ The original enactment of FOIA amended the public disclosure section of the APA. *See EPA v. Mink*, 410 U.S. 73, 79 (1973). FOIA remains codified within the APA at 5 U.S.C. § 552.

⁷ In defense of its APA claim, the plaintiff also cites one case from outside this Circuit. *See* Pl.’s Opp’n at 8 (citing *Or. Natural Desert Ass’n v. Locke*, 572 F.3d 610, 618 (9th Cir. 2009)). At issue in *Locke* was an agency regulation that defined documents responsive to FOIA requests as those within the possession and control of the agency as of the date of the FOIA request. 572 F.3d at 613. The Oregon Natural Desert Association (“ONDA”) argued that this cut-off regulation violated FOIA. *Id.* The district court agreed and awarded attorney’s fees to ONDA. *Id.* On appeal, the agency argued that it should not be liable for ONDA’s attorney’s fees regarding this claim because the claim should have been brought under the APA, not FOIA. *Id.* at 618. The Ninth Circuit did not adopt the agency’s reasoning and held that, even if the claim had been brought under the APA, ONDA would have prevailed in its challenge to the validity of the regulation and would have been awarded attorney’s fees. *Id.*

but rather from the NSA's failure to abide by its own regulations. *See* Pl. Opp'n at 8. This distinction is not persuasive. The plaintiff is requesting the same relief for its APA claim that it is requesting for its FOIA claims – a court order requiring production of all responsive agency records and requiring the NSA to file a *Vaughn* Index describing and justifying all claimed exemptions. *See* Compl., Requested Relief ¶¶ A-B. Accordingly, adequate relief is available under FOIA without recourse to the APA. *See* *Feinman*, 713 F. Supp. 2d at 76-77 (finding relief under the APA precluded when the plaintiff was challenging agency's FOIA procedure, not agency's substantive determinations on his FOIA request, because plaintiff would receive the same relief if he prevailed on his FOIA claims); *see also* *Garcia*, 563 F.3d at 522 (explaining that APA review is precluded where Congress has otherwise provided an adequate alternative remedy that offers relief of the "same genre").

Since adequate relief is available to the plaintiff under FOIA, the Court will grant the defendants' motion to dismiss Count IV of the plaintiff's Complaint.

III. CONCLUSION

For the reasons stated above, the Court concludes that Counts III and IV of the plaintiff's Complaint should be dismissed and that the NSC should be dismissed from this action.

Accordingly, the defendants' partial motion to dismiss is granted. The parties shall submit a joint report on or before July 20, 2011, on the status of this matter and a proposed schedule for completion of a *Vaughn* index and/or dispositive motions. An order consistent with this Memorandum Opinion will be entered separately.

DATED: July 7, 2011

/s/ Beryl A. Howell
BERYL A. HOWELL
United States District Judge

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

_____)	
ELECTRONIC PRIVACY)	
INFORMATION CENTER)	
)	
Plaintiff,)	
)	
v.)	Case No. 1:10-cv-00196-BAH
)	
NATIONAL SECURITY AGENCY)	
)	
)	
)	
Defendant.)	
_____)	

**MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT
OF DEFENDANT’S MOTION FOR SUMMARY JUDGMENT**

PRELIMINARY STATEMENT

The Electronic Privacy Information Center (“EPIC”) brought this Freedom of Information Act (“FOIA”) action to compel the disclosure of National Security Presidential Directive 54 (“NSPD 54”) from the National Security Agency (“NSA”), along with certain allegedly associated documents. NSA has produced all responsive documents (with some limited redactions), with the exception of NSPD 54 which NSA has withheld in its entirety.

As outlined herein and in the declarations attached to this motion, NSA’s withholding of NSPD 54 complies with specific statutory exemptions to FOIA’s disclosure requirement – most relevantly, FOIA Exemption 5, which, among other protections, allows a government agency to withhold a document – like NSPD 54 – that constitutes a confidential presidential communication. NSPD 54 falls within the core of

the presidential communication privilege, which is one of the privileges incorporated into Exemption 5: The document is a direct, confidential communication from the President to senior officials of his administration, on a sensitive topic where disclosure would inhibit the President's ability to engage in effective communication and decisionmaking.

Additionally, certain specific sections of NSPD 54 and the other documents responsive to Plaintiff's FOIA request (documents which were produced with limited redactions) were properly withheld under two other FOIA Exemptions: Exemption 1, which allows the withholding of documents (or portions thereof) that have been properly classified in the interest of national security, and Exemption 3, which allows the withholding of documents (or portions thereof) protected from release by statute.

Because NSA has fully discharged its obligations under FOIA, Defendant respectfully requests that summary judgment be entered in its favor.

I. Background

A. EPIC's FOIA Request

On June 15, 2009, EPIC filed a FOIA request with the NSA (the "FOIA Request"), requesting the following documents:

(1) the text of the National Security Presidential Directive 54 . . . ; (2) the full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation; and (3) any privacy policies related to either the Directive[or] the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative.

B. NSPD 54

As its name indicates, NSPD 54 – the primary document sought by Plaintiff – constitutes direction from the President himself on sensitive and national security topics. The President issued NSPD 54 to communicate his direction on specific actions to be undertaken by the federal government to safeguard federal cybersecurity. He provided this direction to a number of high ranking presidential advisers, Cabinet officials, and agency heads, including (*inter alia*) the Directors of NSA and the Office of Management and Budget, and the Secretaries of State, Defense, Homeland Security, Commerce, and Treasury. Declaration of Mary Ronan (“Ronan Decl.”) ¶ 13. NSPD 54 directs these (and other) officers to take a variety of specific actions towards (*inter alia*) increasing the security of federal government networks, protecting data, and improving the federal government’s capacity to deter and respond to outside threats to federal systems and information. *Id.* NSPD 54 thus collected a variety of specific cybersecurity directives issued by the Presidents to high-ranking officials within the Executive Branch. *See id.*

C. Processing of Plaintiff’s FOIA Request

After various correspondence to and from EPIC (*see* Declaration of Diane M. Janosek (“Janosek Decl.”) ¶¶ 10-17), the NSA (i) produced two documents responsive to the third provision of the FOIA request (with limited redactions), (ii) withheld two draft documents responsive to the third provision of the FOIA request because those documents were non-final and deliberative, and (iii) withheld the NSPD 54 in full. NSA also informed EPIC that it had conducted a reasonable search to locate agency records

responsive to the FOIA Request's second item, but that no responsive additional documents were located. *Id.* ¶ 15.

EPIC filed an administrative appeal challenging certain aspects of NSA's response to the FOIA request (*id.* ¶ 17), and thereafter filed suit on February 4, 2010 challenging (i) the NSA's decision to withhold the two aforementioned draft documents responsive to prong three of the FOIA Request, and (ii) the NSA's decision to withhold NSPD 54.¹ EPIC has not challenged the adequacy or scope of the search for documents responsive to item three of the FOIA Request, nor has EPIC challenged the NSA's withholding of information from the two documents originally produced in response to prong three of the FOIA Request. Additionally, although EPIC's administrative appeal to the NSA challenged "the NSA's failure to disclose any records responsive to part 2 of EPIC's FOIA request" (*see* Complaint ¶ 46), EPIC's Complaint has not challenged this aspect of the NSA's response to item two of the FOIA Request. *See* Complaint ¶¶ 60-63.²

¹ EPIC's Complaint also brought suit against the National Security Council and alleged that NSA's response to the FOIA Request constituted a violation of the Administrative Procedure Act. The United States moved to dismiss these claims. By order of July 7, 2011 ("July 7 Order"), this Court granted the United States' motion and dismissed counts III and IV of the Complaint, thereby leaving only the two claims against the NSA discussed in the instant motion.

² This Court's description of Plaintiff's Complaint confirms that Plaintiff has not affirmatively challenged NSA's response to Item 2 of the FOIA Request. *See* July 7 Order at 4-5 ("In Count I of the Complaint, the plaintiff alleges that the NSA violated FOIA by failing to comply with statutory deadlines regarding its administrative appeal. [Complaint] ¶¶ 52-57. In Count II, the plaintiff alleges that the NSA failed to disclose responsive agency records through (1) withholding records that are not exempt, (2) withholding nonexempt portions of records that are reasonably segregable from exempt portions, and (3) improperly referring a portion of the plaintiff's FOIA request to the NSC. *Id.* ¶¶ 58-63.")

During the pendency of this litigation, NSA finalized the two draft documents (discussed above) that were withheld from production in response to item three of the FOIA Request. Accordingly, the NSA produced those documents to EPIC (with limited redactions) on August 30, 2011. Janosek Decl. ¶ 15 & n.2. The NSA has thus produced all documents that were responsive to item three of the FOIA Request, and Plaintiff has not challenged the scope of NSA's search for documents responsive to item three, or alleged that NSA has failed to disclose any additional documents.

Plaintiff's remaining claims thus largely focus on the decision to withhold NSPD 54. As discussed herein, because NSA complied with its obligations under FOIA with respect to all three sub-sections of the FOIA Request, this Court should grant summary judgment in favor of NSA.

II. Statutory Background and Standard of Review

The Freedom of Information Act, 5 U.S.C. § 552, generally mandates disclosure, upon request, of government records held by an agency of the federal government except to the extent such records are protected from disclosure by one of nine exemptions. The “fundamental principle” that animates FOIA is “public access to Government documents.” *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 151 (1989). “The basic purpose of FOIA 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.” *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978). At the same time, Congress recognized “that legitimate governmental and private interests could be harmed by release of certain types of information and provided nine

specific exemptions under which disclosure could be refused.” *FBI v. Abramson*, 456 U.S. 615, 621 (1982); *see also* 5 U.S.C. § 552(b). While these exemptions are to be “narrowly construed,” *Abramson*, 456 U.S. at 630, courts must not fail to give them “meaningful reach and application.” *John Doe Agency*, 493 U.S. at 152. FOIA thus “represents a balance struck by Congress between the public’s right to know and the government’s legitimate interest in keeping certain information confidential.” *Ctr. for Nat’l Sec. Studies v. U.S. Dep’t of Justice*, 331 F.3d 918, 925 (D.C. Cir. 2003).

“FOIA cases are typically and appropriately decided on motions for summary judgment.” *Moore v. Bush*, 601 F.Supp.2d 6,12 (D.D.C. 2009). Summary judgment is appropriate “if the pleadings, the discovery and disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(c)(1)(C)(2). When a plaintiff challenges an agency’s decision to withhold a document under a FOIA exemption, the agency bears the burden of justifying nondisclosure. *Judicial Watch, Inc. v. Dep’t of Army*, 402 F.Supp.2d 241, 245 (D.D.C. 2005). An agency can meet its burden by submitting declarations or affidavits that describe the documents and justify the basis for nondisclosure with reasonably specific detail. *Military Audit Project v. Casey*, 656 F.2d 724, 738 (D.C. Cir. 1981).

In determining whether an agency has met its burden, Courts review *de novo* the agency’s use of a FOIA exemption to withhold documents. *Wolf v. CIA*, 473 F.3d 370, 374 (D.C. Cir. 2007). “[S]ummary judgment is warranted on the basis of agency affidavits when the affidavits describe the justifications for nondisclosure with reasonably

specific detail . . . and are not controverted by either contrary evidence in the record nor by evidence of agency bad faith.” *Wolf*, 473 F.3d at 374 (internal quotation marks omitted) (omission in original). “Ultimately, an agency’s justification for invoking a FOIA exemption is sufficient if it appears ‘logical’ or ‘plausible.’” *Id.* at 374-75.

ARGUMENT

I. NSPD 54 is a Confidential Presidential Communication and is Therefore Entirely Exempt From Disclosure Under FOIA Exemption 5

NSPD 54 constitutes a confidential presidential communication and is therefore exempt from disclosure under FOIA Exemption 5.

Exemption 5 exempts from mandatory disclosure “inter-agency or intra-agency memorandums or letters which would not be available by law to a party . . . in litigation with the agency.” 5 U.S.C. § 552(b)(5). In particular, it “exempts those documents . . . that are normally privileged in the civil discovery context.” *NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 149 (1975). Exemption 5 thus incorporates the privileges available in civil discovery and allows NSA to withhold privileged documents from production. *See id.*

Among other privileges, the D.C. Circuit has repeatedly held that Exemption 5 incorporates the presidential communications privilege, which is rooted in separation of powers concerns and has been recognized since the earliest days of the United States. *See, e.g., United States v. Nixon*, 418 U.S. 683, 708 (1974) (describing presidential communications privilege as “fundamental to the operation of Government and inextricably rooted in the separation of powers under the Constitution”); *see also In re*

Sealed Case, 121 F.3d 729, 745 (D.C. Cir. 1997); *Judicial Watch v. Department of Justice*, 365 F.3d 1108, 1113 (D.C. Cir. 2004). The privilege applies to “communications in performance of a President’s responsibilities, . . . and made in the process of shaping policies and making decisions.” *Nixon v. Administrator of General Services*, 433 U.S. 425, 449 (1997) (internal citations and formatting omitted).³

This case involves application of the established principle that “communications directly involv[ing] the President . . . are entitled to the privilege” because of the need to protect the President’s ability “to make decisions confidentially.” *Loving*, 550 F.3d at 40 (internal citations omitted); *Citizens for Responsibility & Ethics v. United States Dep’t of Homeland Sec.*, 514 F. Supp. 2d 36, 49-50 (D.D.C. 2007) (“The core of the presidential communications privilege is the protection of the President’s need for confidentiality in the communications of his office.” (internal citations omitted)).

The privilege “covers final and post-decisional materials” as well as deliberative ones. *In re Sealed Case*, 121 F.3d at 745. Such final documents “often will be revelatory of the President’s deliberations” especially where such documents both embody presidential direction as to “a particular course of action,” while also “ask[ing] advisers to submit follow-up reports so that [the President] can monitor whether this course of action is likely to be successful.” *In re Sealed Case*, 121 F.3d at 745-746. The D.C. Circuit has sensibly applied the presidential communications privilege to final and post-decisional

³ Documents subject to the presidential communications privilege are shielded in their entirety. *See, e.g., Loving v. DOD*, 550 F.3d 32, 37-38 (D.C. Cir. 2008) (“The privilege covers documents reflecting presidential decisionmaking and deliberations . . . and it covers the documents in their entirety.” (internal citations omitted)); *Judicial Watch*, 365 F.3d at 1114; *In re Sealed Case*, 121 F.3d at 745.

documents because “limit[ing] the President’s ability to communicate his decisions privately” would “interfere[e] with his ability to exercise control over the executive branch.” *In re Sealed Case*, 121 F.3d at 745-746.

Because NSPD 54 is a confidential post-decisional communication from the President to senior officials of his administration, the presidential communications privilege squarely applies in this case, thereby relieving NSA of any obligation to disclose NSPD 54. Detailed descriptions of NSPD 54 are set out in the attached Janosek Declaration and Ronan Declaration, which explain why the presidential communications privilege applies to NSPD 54 and justifies withholding it in its entirety.

First, NSPD 54 embodies communications directly from the president. Janosek Decl. ¶¶ 8, 31; Ronan Decl. ¶¶ 7, 13. As the Ronan Declaration makes clear, NSPD 54 was issued by the President and solicits feedback in order to assist the President’s ability to oversee implementation of his directives. Ronan Decl. ¶ 13. As discussed above, the presidential communications privilege squarely applies to communications, such as these, that directly involve the President and that solicit responses designed to aid the President’s ability to monitor implementation efforts. *See, e.g., In re Sealed Case*, 121 F.3d at 745-746; *see also Loving*, 550 F.3d at 40.

Second, NSPD 54 was communicated to top presidential advisors and cabinet officials. As described in the Ronan declaration, NSPD 54 embodied directives to the director of the Office of Management and Budget, the President’s National Security Staff, various cabinet officials, and other top presidential assistants. Ronan Decl. ¶ 13. At its core, the presidential communications privilege is meant to protect exactly this type of

communication: High level communications between the President and his highest ranking advisors and officials of his administration, which present the greatest need for confidential, unencumbered dialog. *See, e.g., Judicial Watch*, 365 F.3d at 1116-17.

Third, the NSPD 54 is a confidential communication. The President has explicitly sought to maintain the confidentiality of the decisions embodied in NSPD 54 and, relatedly, has solicited confidential feedback in return. As the Ronan Declaration makes clear, the memorandum accompanying NSPD 54 stressed the confidentiality of NSPD 54, and prohibited dissemination of the document beyond its authorized recipients without White House the approval of the White House and further instructed that even within receiving agencies, copies should be distributed only on a need to know basis. Ronan Declaration ¶ 7; *see also* Janosek Declaration ¶¶ 32-33 (discussing confidentiality of NSPD 54 and limitations on its distribution). As the D.C. Circuit has repeatedly held, the presidential communications privilege applies where (as here) the President concludes that a document embodying his directives needs to remain confidential. *Judicial Watch*, 365 F.3d at 1113-1114 ; *In re Sealed Case*, 121 F.3d at 744. And NSPD 54's request for confidential reporting back to the President (Ronan Declaration ¶ 13) likewise underscores the necessity of privilege in this case because disclosure of the President's requests to have "his advisers . . . submit follow-up reports" would "limit the President's ability to communicate his decisions privately, thereby interfering with his ability to exercise control over the executive branch." *In re Sealed Case*, 121 F.3d at 745-746. Thus, the President's various efforts to keep NSPD 54 confidential support the application of the privilege in this case.

As noted above, where the presidential communications privilege applies, the entire document is exempt from disclosure. *See, e.g., Loving v. DOD*, 550 F.3d at 37-38; *Judicial Watch*, 365 F.3d at 1114; *In re Sealed Case*, 121 F.3d at 744. Thus, because NSPD 54 embodies various confidential directives from the President to high ranking executive officials, and because the document likewise solicits confidential feedback from these same officials directly to the President, the entire document was properly withheld under the presidential communications privilege.

Although Exemption 5 does not require a showing of harm to sustain a claim of presidential communication privilege, *see, e.g., McKinley v. Bd. of Governors of the Fed. Reserve Sys.*, 647 F.3d 331 (D.C. Cir. 2011); *Quarles v. Department of Navy*, 893 F.2d 390, 393 (D.C. Cir. 1990), the release of NSPD 54 would, in fact, result in specific harm to the President and his top advisers. Disclosure of NSPD 54 would implicate the core concerns underlying the presidential communication privilege because it would inhibit the fully informed and candid deliberation within the White House and the Executive Branch that is necessary to enable the President to fulfill his duties as Commander in Chief and as Chief Executive. Ronan Decl. ¶ 14. Release of NSPD 54 would impair the President's ability to effectively communicate directives to top advisers and to solicit feedback in response – both on issues of cybersecurity and on all other issues requiring confidential Executive Branch communication. *Id.*

Beyond the harms to presidential communication generally, release of NSPD 54 would undermine the very cybersecurity efforts that the document sought to promote: communications between the President and high ranking Executive Branch advisers and

cabinet officials on the security of federal network assets. As described herein, NSPD 54 employs a confidential process to direct high ranking federal officials to assess and take certain specific actions with respect to cybersecurity, and also tasks these same federal officials with submitting confidential reports on cybersecurity efforts directly back to the President. Disclosure of such efforts would undermine federal cybersecurity by alerting the United States' adversaries to aspects of the very capabilities of federal cyberspace that the President sought to protect through NSPD 54. More generally, disclosure of NSPD 54 would undermine the ability of federal officials to communicate effectively on efforts to promote cybersecurity – a confidential process that the President deemed critical to achieving the purposes of NSPD 54.

Accordingly, because NSPD 54 constitutes presidential communication of a type that is exempt from mandatory disclosure under FOIA, the Court should enter summary judgment for defendant.

II. Sections of NSPD 54 Are Properly Classified and Therefore Exempt From Disclosure Under FOIA Exemption 1

In addition to the presidential communication privilege – which, as discussed above, allows the withholding of NSPD 54 in its entirety – certain sub-sections of NSPD 54 are protected from disclosure under FOIA Exemption 1.

Exemption 1 protects records that are: “(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order.” 5 U.S.C. § 552(b)(1). Several provisions of NSPD 54 are properly classified under

Executive Order 13526 and meet both of the requirements for nondisclosure under Exemption 1.

Given the significance of classified information, courts are particularly deferential to classification decisions by the executive branch. As uniformly recognized by courts, classification decisions are entitled to “substantial weight.” *See, e.g., Larson v. Dep’t of State*, 565 F.3d 857, 864 (D.C. Cir. 2009). Moreover, it is not appropriate for courts to substitute their judgment for that of the executive with regard to classified information. *See Larson*, 565 F.3d at 865; *Halperin v. CIA*, 629 F.2d 144, 148 (D.C. Cir. 1980) (“Judges . . . lack the expertise necessary to second-guess such agency opinions in the typical national security FOIA case.”). As a result, the D.C. Circuit has held that “the text of Exemption 1 itself suggests that little proof or explanation is required beyond a plausible assertion that information is properly classified.” *Morley v. Cent. Intelligence Agency*, 508 F.3d 1108, 1124 (D.C. Cir. 2007).

Under Executive Order 13526, information may be classified if it meets the following conditions:

- (1) an original classification authority is classifying the information;
- (2) the information is owned by, produced by or for, or is under the control of the United States Government;
- (3) the information falls within one or more of the categories of information listed in section 1.4 of this order; and
- (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security,

which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

Executive Order 13526, Section 1.1. The classified provisions of NSPD 54 meet each of these conditions and therefore have been properly classified and are exempt from disclosure.

First, Ms. Ronan, Director of the Access Management Office for the National Security Staff (NSS), has authority to classify and declassify national security information, has personally reviewed the classified material, and has determined that it has been properly classified under Executive Order 13526. Ronan Decl. ¶ 1-12.

Second, Ms. Ronan has concluded that the release of the information classified as “SECRET” could reasonably be expected to cause serious damage to the national security and that the release of the information classified as “TOP SECRET” could reasonably be expected to cause exceptionally grave damage to the national security. *Id.* ¶ 11.

Third, the classified material falls within the categories of classifiable information listed in section 1.4 of Executive Order 13526. Executive Order 13526 provides that information shall not be considered for classification unless it falls within one (or more) of eight specifically enumerated categories of information. The Ronan declaration makes clear the relevant sections of NSPD 54 have been properly classified under Sections 1.4(c), because they involve intelligence activities or intelligence sources and methods; 1.4(d), because they involve foreign relations or foreign activities of the United States; 1.4(e), because they involve scientific, technological, or economic matters relating to the national security; and 1.4(g), because they involve vulnerabilities or capabilities of

systems, installations, infrastructures, projects, plans, or protection services relating to the national security. Ronan Decl. ¶ 11.

Thus, the classified material within NSPD 54 is properly exempt from disclosure under FOIA Exemption 1.

III. The NSA Properly Redacted Two Documents Responsive to the Third Item in the FOIA Request Pursuant to FOIA Exemptions 1 and 3

Under FOIA Exemptions 1 and 3, NSA properly withheld the redacted portions of NSA Policy 1-58 and IAD Management Directive 20 – the two documents produced during NSA’s Supplemental Production as responsive to the third item in the FOIA Request (the “Item Three Documents”).

A. Material Redacted from NSA Policy 1-58 is Properly Classified and Therefore Exempt from Disclosure under FOIA

The NSA properly withheld from production material within NSA Policy 1-58 that is classified and therefore exempt from disclosure under FOIA Exemption 1.

As discussed above, Exemption 1 protects records that are properly classified. Redacted material within NSA Policy 1-58 is properly classified as “secret” under Executive Order 13526 and meets the requirements for nondisclosure under Exemption 1. The conditions for classification are provided by Executive Order 13526 and, as described above, require classification by an original classification authority, require the classified information to fall within one of the categories of information provided by Section 1.4 of Executive Order 13525, and require a determination that the unauthorized disclosure of the information reasonably could be expected to result in damage to the

national security. Executive Order 13526, Section 1.1. The classified material within NSA Policy 1-58 meets each of these conditions and has been properly classified.

First, Ms. Janosek, Deputy Associate Director for Policy and Records for the National Security Agency, has authority to classify and declassify national security information, has personally reviewed the redacted material, and has determined that it has been properly classified under Executive Order 13526. Janosek Decl. ¶ 1, 19-23. Ms. Janosek has further concluded that the release of this information could reasonably be expected to cause serious damage to the national security. *Id.* ¶ 20.

Second, the redacted material falls within the categories of classifiable information listed in section 1.4 of Executive Order 13526. As discussed above, Executive Order 13526 provides that information shall not be considered for classification unless it falls within one (or more) of eight specifically enumerated categories of information. Among its other provisions, Section 1.4 allows for the classification of documents embodying information regarding foreign governments (Section 1.4(b)), intelligence activities (including covert action), intelligence sources and methods, or cryptology (Section 1.4(c)), and vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security (Section 1.4(g)).

The Janosek Declaration makes clear that the material redacted from NSA Policy 1-58 – embodying operational details of NSA’s implementation of NSPD 54 – was properly classified because it included information on these three various topics. The information in NSA/CSS Policy 1-58 that was withheld under Exemption 1 would, if released, reveal (among other things) operational details of NSA’s implementation of the

NSPD 54. Janosek Decl. ¶¶ 19, 22-23. Ms. Janosek states that the release of this information would in turn reveal information about NSA's capabilities and limitations, thereby rendering the material appropriately classified under Sections 1.4(c) and 1.4(g).
Id.

The Janosek Declaration also demonstrates that release of the redacted information would disclose the methodology used by NSA to respond to cyber-threats, disseminate warning information, assist DHS in the performance of its cyber-mission, ensure the security of US government national cyber systems, and protect the security of federal systems from adversaries. Because revelation of this type of information could help identify vulnerabilities in U.S. assets (Janosek Decl. ¶¶ 21-23), the information was properly classified and redacted under Section 1.4 and FOIA Exemption 1.

B. The NSA Also Properly Redacted Material from the Item Three Documents Under Exemption 3

NSA has also properly invoked Exemption 3, which covers records that are “specifically exempted from disclosure” by another federal statute “if that statute—establishes particular criteria for withholding the information or refers to the particular types of material to be withheld.” 5 U.S.C. § 552(b)(3).

In promulgating FOIA, Congress included Exemption 3 to recognize the existence of collateral statutes that limit the disclosure of information held by the government, and to incorporate such statutes within FOIA's exemptions. *See Baldrige v. Shapiro*, 455 U.S. 345, 352-53 (1982); *Essential Info., Inc. v. U.S. Info. Agency*, 134 F.3d 1165, 1166 (D.C. Cir. 1998). Under Exemption 3, “the sole issue for decision is the existence of a

relevant statute and the inclusion of withheld material within the statute's coverage.”

Fitzgibbon v. CIA, 911 F.2d 755, 761-62 (D.C. Cir. 1990). Thus, if another statute is recognized as providing a basis for invoking Exemption 3, an agency is *per se* authorized to withhold material falling within the scope of that statute.

The Janosek Declaration supports the “two-part inquiry [that] determines whether Exemption 3 applies to a given case.” *Minier v. CIA*, 88 F.3d 796, 800-01 (9th Cir. 1996) (citing *CIA v. Sims*, 471 U.S. 159, 67 (1985)). “First, a court must determine whether there is a statute within the scope of Exemption 3. Then, it must determine whether the requested information falls within the scope of the statute.” *Id.*

Several statutes provide explicit bases for the withholdings from the Item Three Documents. Section 6 of the National Security Agency Act of 1959, Public Law 86-36 (50 U.S.C. § 402 note) (“Section 6”), exempts the NSA from disclosing its operational details. Section 6 provides that “[n]othing in . . . any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, [or] of any information with respect to the activities thereof.” (Emphasis added). The D.C. Circuit has repeatedly held Section 6 “to be an Exemption 3 statute.” *See, e.g., Hayden v. National Sec. Agency/Central Sec. Service*, 608 F.2d 1381, 1389 (D.C. Cir. 1979). Thus, Exemption 3 properly allows for the withholding of any material relating to NSA Operations.

In specifically exempting NSA operational information from the requirements of other disclosure laws (including FOIA), Congress recognized, as a matter of law, the potential and serious harm that might arise from the disclosure of any information

relating to NSA activities. *Hayden v. NSA*, 608 F.2d 1381, 1390 (D.C. Cir. 1979); *Larson v. Department of State*, 565 F.3d 857, 868 (D.C. Cir. 2009); *Students Against Genocide v. Department of State*, 257 F.3d 828 (D.C. Cir. 2001); *People for the American Way v. NSA*, 462 F.Supp.2d 21, 30 (D.D.C. 2006). But, in any event, “[a] specific showing of potential harm to national security . . . is irrelevant to the language of [Section 6 because] Congress has already, in enacting the statute, decided that disclosure of NSA activities is potentially harmful.” *Hayden*, 408 F.2d at 1390.

The protection provided by this statutory privilege is, by its very terms, absolute, and “must be construed to prohibit the disclosure of information relating to NSA's functions and activities as well as its personnel.” *See, e.g., Linder v. NSA*, 94 F.3d 693 (D.C. Cir. 1996). Section 6 states unequivocally that, notwithstanding any other law, including FOIA, NSA cannot be compelled to disclose *any* information with respect to its activities. *See Hayden*, 608 F.2d at 1389. To invoke this privilege, NSA must demonstrate only that the information it seeks to protect falls within the scope of Section 6. “[A]ll that is necessary for the [NSA] to meet its burden under Public Law No. 86-36 and Exemption 3” is support in a declaration that the “requested documents concern[] a specific NSA activity, to wit, intelligence reporting based on electromagnetic signals.” *Id.* at 1390.

Two other statutes provide overlapping bases for withholding information under FOIA. First, 18 U.S.C. § 798 prohibits the unauthorized disclosure of classified information (i) concerning the communications intelligence activities of the United States or (ii) obtained by the process of communication intelligence derived from the

communications of any foreign government. In exempting “communications intelligence” from disclosure, this statute allows the withholding of any information regarding procedures and methods used in the interception of communications and the obtaining of information from such communications.

Similar protection is provided by Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 403-1(i)(1), which protects “intelligence sources and methods from unauthorized disclosure, including NSA sources and methods. Janosek Decl. ¶ 27. Like the protection afforded to core NSA activities by Section 6 of the NSA Act of 1959, the protection afforded to intelligence sources and methods is absolute. *See Central Intelligence Agency v. Sims*, 471 U.S. 159 (1985). Whether the sources and methods at issue are classified is irrelevant for purposes of the protection afforded by 50 U.S.C. § 403-1(i)(1). *Id.*

The information redacted from the Item Three Documents is definitively exempted from disclosure on the basis of the statutes described above. The redacted material addresses how NSA implements NSPD 54’s cybersecurity related directives (Janosek Decl. ¶ 28) – information that self-evidently relates to the operation of the NSA (and is therefore exempt from disclosure under Section 6) and that also is exempted from disclosure from the other statutes discussed above.

The NSA’s implementation of NSPD 54 directly relates to core agency functions – assisting in the protection of U.S. information systems. *Id.* Revealing the material redacted from the Item Three Documents would explicitly reveal certain techniques used

by NSA to protect these information systems; a methodology exempt from disclosure under Section 6.

Likewise, the information also directly relates to NSA efforts to collect, process, analyze, and disseminate signals intelligence information for national foreign intelligence and counterintelligence purposes. *Id.* ¶¶ 3, 28. Section 6 provides absolute protection to such NSA operational information. Accordingly, all of the information withheld in NSA/CSS Policy 1-58 and IAD Management Directive 20 is exempt pursuant to Exemption 3 based on Section 6 alone.

Additionally, some of the same information that is exempt based on Section 6 is also exempt under Exemption 3 (i) based on 18 U.S.C. § 798, because disclosure would reveal classified information derived from NSA's exploitation of foreign communications; and (ii) under 50 U.S.C. § 403-1(i)(1), because the information concerns intelligence sources and methods – specifically, as discussed above, the sources and methods used by the NSA to collect and evaluate signals intelligence. *Id.* ¶ 29.⁴

IV. The NSA Conducted a Reasonable Search for Documents Responsive to Item Two of the FOIA Request

NSA's search for records responsive to item number two of the FOIA request – seeking “the full text, including previously unreported sections, of the Comprehensive

⁴ Similarly, separate and apart from the invocation of the presidential communications privilege over NSPD 54 and the classification exemption asserted in the Ronan Declaration, the NSA has invoked Exemptions 1 and 3 with respect to one paragraph of NSPD 54 that relates to the operations of the NSA and contains classified material. This material is exempt from disclosure for the same reasons discussed herein: It has been properly classified and, in speaking to the operations of the NSA, it is excepted from disclosure by Section 6 and the other statutes discussed above. *See* Janosek Decl. ¶ 34.

National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation” – was reasonably calculated to uncover all documents responsive to that request and therefore provides a sufficient basis for granting summary judgment as to item two of the FOIA Request.

As an initial matter, it bears noting that Plaintiff has not challenged NSA’s response to this item of the FOIA Request. As discussed above, NSA informed EPIC that its reasonable search had not uncovered agency records responsive to the second prong of EPIC’s request. Janosek Decl. ¶ 15. Although EPIC’s administrative appeal challenged this determination (Complaint ¶ 46), EPIC’s complaint in this litigation has not challenged the NSA’s response to item two of the FOIA Request. *See* Complaint ¶¶ 60-63; *see also* July 7 Order at 4-5.

In any event, even if Plaintiff’s Complaint could be deemed to challenge the NSA’s response to Item Two, such a challenge should be dismissed.

Where a plaintiff challenges the adequacy of an agency’s search, an agency must demonstrate “that it made a good faith effort to conduct a search for the requested records, using methods which can be reasonably expected to produce the information requested.” *Oglesby v. U.S. Dep’t of the Army*, 920 F.2d 57, 68 (D.C. Cir. 1990) (citations omitted). According to the D.C. Circuit, “the issue . . . is not whether there might exist any other documents possibly responsive to the request, but rather whether the search for those documents was adequate.” *Weisberg v. Dep’t of Justice*, 745 F.2d 1476, 1485 (D.C. Cir. 1984) (emphasis and citations omitted). In evaluating the adequacy of a search, courts will accord agency affidavits “a presumption of good faith,

which cannot be rebutted by purely speculative claims about the existence and discoverability of other documents.” *SafeCard Servs., Inc. v. SEC*, 926 F.2d 1197, 1200 (D.C. Cir. 1991); *see also Ground Saucer Watch, Inc. v. CIA*, 692 F.2d 770, 771 (D.C. Cir. 1981). The statute does not require “meticulous documentation [of] the details of an epic search.” *Perry v. Block*, 684 F.2d 121, 127 (D.C. Cir. 1982).

Item Two essentially seeks two categories of information: (1) “the full text . . . of the Comprehensive National Cybersecurity Initiative” (“CNCI”) and (2) “executing protocols distributed to the agencies in charge of” the CNCI’s implementation. In response to Item Two, the NSA conducted comprehensive searches in June and July 2009 within the relevant Signal Intelligence Directorate and Information Assurance Directorate organizations – the subdivisions of the NSA plausibly responsible for implementing aspect of the CNCI – searching for any potentially responsive documents. Janosek Decl. ¶ 36.

The full text of the CNCI is embodied in NSPD 54. *Id.* Accordingly, the full text of the CNCI was properly withheld along with the remainder of NSPD 54 for the various reasons discussed above.

Otherwise, Item Two seeks “executing protocols distributed to the agencies in charge of” the CNCI’s implementation. Per the plain terms of the FOIA Request, NSA searched for documents that were “distributed to” the NSA – meaning, documents originating outside the NSA – that detailed “executing protocols” for the CNCI. *Id.* ¶ 36. As stated in the Janosek declaration, NSA identified the organizations within NSA which would be responsible for executing aspects of the CNCI (which included the Signal

Intelligence Directorate and the Information Assurance Directorate), and asked those NSA components to search all files for documents distributed to NSA on how to execute the CNCI. *Id.* ¶¶ 36-37. Although these same NSA components searched for and produced records responsive to item number three of the FOIA Request, the reasonable search related to Item Two did not result in the location of any responsive documents (other than NSPD 54 itself). *Id.*

In its administrative appeal, EPIC argued that, in light of their assessment of NSA's involvement in NSPD 54, "it is very unlikely that a truly 'thorough search' by the NSA would fail to turn up a single record satisfying request part 2." *Id.* ¶ 17, Ex. G at 6. But the absence of any documents (outside of NSPD 54) is not surprising. In light of the confidential treatment demanded of NSPD 54 and the presidential dictates embodied in NSPD 54 itself, there is no reason to expect that the NSA would have been supplied with *additional* protocols for executing this confidential document; the directives of the President were presumably sufficient.

In any event, EPIC's speculation as to whether such documents should reasonably exist is irrelevant. The adequacy of NSA's search must be determined not by its results, "but by the appropriateness of the methods used to carry out the search." *Iturralde v. Comptroller of Currency*, 315 F.3d 311, 315 (D.C. Cir. 2003) (citing *Steinberg v. Dep't of Justice*, 23 F.3d 548, 551 (D.C. Cir. 1994)). As the D.C. Circuit has held, a plaintiff cannot escape summary judgment simply by speculating as to "records whose existence remains purely hypothetical" because such claims "cannot be conclusively refuted, since to do so the government would have to prove a negative – that the files in question do not

exist.” *Meeropol v. Meese*, 790 F.2d 942 (D.C. Cir. 1986). Just so here: Plaintiff’s unfounded assumption “that a particular subject was of such importance that a [document] on that subject must have been created” (*id.*) provides an insufficient basis for challenging the reasonableness of an agency’s search.

As discussed above, the D.C. Circuit has made clear that an agency declaration provides a sufficient basis for summary judgment absent contrary evidence or evidence of bad faith by the agency. *Wolf*, 473 F.3d at 374. EPIC has submitted no evidence suggesting that NSA’s search was not reasonably calculated to uncover the externally-generated executing protocols sought by Item Two of the FOIA Request; its conclusory allegations are therefore insufficient to defeat a motion for summary judgment. Accordingly, the Janosek Declaration’s description of the NSA search demonstrates that the NSA complied with its obligations under FOIA and provides a sufficient basis for granting summary judgment here.

CONCLUSION

For the reasons discussed herein, this Court should grant summary judgment to the NSA and dismiss Plaintiff’s action in its entirety.

DATED: October 11, 2011

Respectfully submitted,

TONY WEST
Assistant Attorney General

RONALD C. MACHEN
United States Attorney

ELIZABETH J. SHAPIRO
Deputy Branch Director

/s/Joshua Wilkenfeld
JOSHUA WILKENFELD
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W.
Washington, D.C. 20530
Tel: (202) 305-7920
Fax: (202) 616-8470
Email: joshua.i.wilkenfeld@usdoj.gov

Counsel for Defendants

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

ELECTRONIC PRIVACY)	
INFORMATION CENTER)	
)	
Plaintiff,)	
)	
v.)	Civil Action 10-0196 (BAH)
)	
NATIONAL SECURITY AGENCY,)	
)	
Defendant.)	

DECLARATION OF DIANE M. JANOSEK

I, DIANE M. JANOSEK, hereby declare and state:

1. I am the Deputy Associate Director for Policy and Records for the National Security Agency (hereinafter, "NSA" or "Agency"). I have served with NSA for over eleven (11) years, and prior to my current assignment, I held various leadership positions throughout the Agency. As the Deputy Associate Director for Policy and Records, I am responsible for processing all requests made pursuant to the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552 (2006), as amended by the OPEN Government Act of 2007, Pub. L. No. 110-175. I am also a TOP SECRET classification authority pursuant to section 1.3 of Executive Order 13526. It is my responsibility to assert/invoke FOIA exemptions in the course of litigation. Through the exercise of my official duties as Deputy Associate Director for Policy and Records, I have become familiar with the current litigation arising of the request for records filed by Plaintiff, the Electronic Privacy Information Center, under the FOIA.

2. The purpose of this declaration is to advise the Court that NSA withheld certain information in the documents that were responsive to the Plaintiff's FOIA request, as set forth below, because the information is properly exempt from release under the FOIA based on Exemptions 1 and 3, 5 U.S.C. §§552(b)(1) and (3), respectively¹. Exemptions 1 and 3 apply because the redacted information is currently and properly classified in accordance with E.O. 13526 and protected from release by statutes, specifically Section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 402 note (Pub. L. 86-36); 18 U.S.C. §798; and Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. §403-1(i)(1). This declaration also advises the Court of the search for records responsive to item #2 of the Plaintiff's request and that NSA did not locate responsive records. In order to provide the necessary context for the discussion that follows, I will describe NSA's origin and mission.

ORIGIN AND MISSION OF NSA

3. NSA was established by Presidential Directive in October 1952 as a separately organized agency within the Department of Defense. See Executive Order 12333 (as amended by Executive Order 13470 (2008)), section 1.7(c). NSA's cryptologic mission has two main missions: (1) to collect, process, analyze, and disseminate Signals Intelligence (SIGINT) information for national foreign intelligence and counterintelligence purposes; and (2) to conduct information security activities.

4. In performing its SIGINT mission, NSA exploits foreign electromagnetic signals to obtain intelligence information necessary to the national defense, national

¹ Exemption 5 is being invoked to withhold National Security Presidential Directive 54 in its entirety because the information in that document embodies confidential presidential communications of a type that are protected by disclosure under the presidential communications privilege. See Ronan Declaration (attached with the Defendant's Memorandum in Support of its Motion for Summary Judgment).

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

5. There are two primary reasons for gathering and analyzing intelligence information. The first, and most important, is to gain the information required to direct U.S. resources as necessary to counter threats. The second reason is to obtain the information necessary to direct the foreign policy of the United States. Foreign intelligence information provided by the NSA is routinely distributed to a wide variety of senior Government officials, including the President; the President's National Security Advisor; the Director of National Intelligence; the Secretaries of Defense, State, Treasury and Commerce; U.S. ambassadors serving in posts abroad; the Joint Chiefs of Staff; and the Unified and Sub-Unified Commanders. In addition, SIGINT information is disseminated to numerous agencies and departments, including, among others, the Central Intelligence Agency; the Federal Bureau of Investigation; the Drug Enforcement Administration; the Departments of the Army, Navy, and Air Force; and various intelligence components of the Department of Defense. Information provided by NSA is relevant to a wide range of important issues, including, but not limited to, military order of battle; threat warnings and readiness; arms proliferation; terrorism; and foreign aspects of international narcotics trafficking. This information is often critical to the formulation

of U.S. foreign policy and the support of U.S. military operations around the world.

Moreover, intelligence produced by NSA is often unobtainable by other means.

6. NSA's ability to produce foreign intelligence information depends on its access to foreign and international electronic communications. Further, SIGINT technology is both expensive and fragile. Public disclosure of either the capability to collect specific communications or the substance of the information itself can easily alert targets to the vulnerability of their communications. Disclosure of even a single communication holds the potential of revealing the intelligence collection techniques that are applied against targets around the world. Once alerted, SIGINT targets can easily frustrate SIGINT collection by using different or new encryption techniques, disseminating disinformation, or by utilizing a different communications link. Such evasion techniques may inhibit access to the target's communications and, therefore, deny the United States access to information crucial to the defense of the United States both at home and abroad.

7. The NSA's Information Assurance mission has as its essence the protection of national security and Department of Defense systems, and direct support to other U.S. government agencies that help protect other U.S. government systems and the U.S. critical infrastructure and key resources. NSA must maintain its formidable advantage to ensure that the United States and its allies can thwart our adversaries who seek to disrupt and exploit our networks and systems by improving the security of our critical operations and information. NSA has an unrivaled awareness of threats to national security systems and how to mitigate them. NSA is simply the standard bearer of government vulnerability discovery and security testing, and provides or oversees cryptography for

national security systems. NSA is also central to public-private initiatives for technology certification, trust engineering, cross-domain solutions, security automation standards, best security practices, information assurance education, and operations security.

NSA/CSS's ROLE IN NSPD 54 AND THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE (CNCI)

8. On 8 January 2009, the President signed the Cybersecurity Policy Presidential Directive (NSPD-54 and HSPD-23). The directive was issued directly by the President, to various Cabinet officials and members of the President's senior staff. The directive included specific directions to high ranking government officials to take discrete steps with regard to cybersecurity. NSPD 54 also implemented the CNCI. Due to the sensitivity of the Presidential policy contained within it, this Directive cannot be disseminated beyond its authorized recipients without the approval of the White House. Even further dissemination within the agencies and departments that received a copy of NSPD 54 is restricted based on a need to know basis.

9. NSA/CSS has a role in the CNCI, but any operational or amplifying details are properly and currently classified in accordance with E.O. 13526 and/or protected from release by statute, specifically, Section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 402 note (Pub. L. 86-36); 18 U.S.C. §798; and/or Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. §403-1(i)(1).

PROCESSING OF PLAINTIFF'S FOIA REQUEST

10. Plaintiff filed a FOIA request on 25 June 2009, which was received by NSA on 26 June 2009, seeking information on the following: (1) The text of the National Security Presidential Directive 54 otherwise referred to as The Homeland Security Presidential Directive 23; (2) The full text, including previously unreported sections, of

the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to agencies in charge of its implementation; and (3) Any privacy policies related to the either the Directive, the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative. Tab A. In this request, the Plaintiff also sought expedited processing and “news media” status. Tab A.

11. By letter dated 1 July 2009, the Chief, FOIA/PA Office, NSA/CSS, responded to Plaintiff’s FOIA request. Tab B. In this initial response, NSA informed Plaintiff that its request for a waiver of fees was granted. Tab B. NSA also informed Plaintiff that its request for expedited treatment was denied and that NSA would process the Plaintiff’s request in NSA’s normal processing queue. Tab B. Because NSA denied Plaintiff’s request for expedited processing, the NSA informed Plaintiff of its right to appeal this determination. Tab B.

12. By letter dated 30 July 2009, Plaintiff appealed NSA’s decision to deny it expedited processing. Tab C. By letter dated 12 August 2009, NSA’s FOIA/PA Appeals Authority granted Plaintiff’s request for expedited processing based on his review of Plaintiff’s original request, the FOIA/PA Office’s initial response, and the information provided by Plaintiff on appeal. Tab D. Accordingly, Plaintiff’s FOIA request was placed in the Agency’s expedite queue, which is one of NSA’s six queues maintained by NSA’s FOIA Office. See 32 C.F.R. §299.5(d).

13. By letter dated 14 August 2009, the NSA FOIA Office informed the Plaintiff that its request was placed in the expedite queue and that NSA had finished its search for

records responsive to its request. Tab E. NSA's FOIA Office informed Plaintiff that two documents (USSID SP0018 and NSA/CSS Policy 1-23) which were responsive to item #3 of its request had been previously released under the FOIA with redactions and that NSA was providing these documents to the Plaintiff as they were approved for release under the FOIA. Tab E. NSA's FOIA Office further informed Plaintiff that if it wanted NSA to conduct a new review of these two previously documents, then it should notify NSA's FOIA Office. Tab E. NSA's FOIA office then explained why certain information in these two documents was withheld in the prior FOIA partial releases. Tab E. Further, NSA's FOIA Office notified Plaintiff as to its right to appeal the withholding of information in these two documents. Finally, the FOIA Office informed Plaintiff that the remaining responsive information had been assigned for review to determine what information could be released and that NSA would finish this review as expeditiously as possible. Tab E.

14. Plaintiff did not request that NSA re-review these two documents nor did Plaintiff appeal the withholdings in the two documents that NSA released by letter dated 14 August 2009.

15. By letter dated 26 October 2009, NSA's FOIA Office informed Plaintiff that it had completed its processing of Plaintiff's FOIA request. Tab F. In this letter, NSA informed Plaintiff that it had conducted a thorough search of its files, but it could not locate any records responsive to item #2 of Plaintiff's request. Tab F. NSA further informed Plaintiff that it had located 3 documents consisting of 26 pages that were response to items # 1 and 3 of Plaintiff's request. Tab F. Specifically, regarding item #3,

NSA informed Plaintiff that there were two responsive documents², but they would be withheld in their entirety based on the fifth exemption of the FOIA because the information contained in these two documents were covered by the deliberative process privilege. Tab F. Additionally, information in both documents was exempt from release based on the third exemption of the FOIA because the information was protected from release by statute. Tab F. Further, information in one of these two documents was also exempt based on the first exemption of the FOIA because the information was currently and properly classified in accordance with the governing executive order. Tab F. Finally, NSA informed Plaintiff that there was one document that was responsive to item #1 of its request, but this document was not an NSA record; rather, the document originated with the National Security Council. Tab F. NSA informed Plaintiff that it had forwarded this document to the National Security Council for a release determination. Tab F.

16. In this letter, NSA also provided Plaintiff with its right to appeal NSA's determinations that there were no documents responsive to item #2 of its request, and its determination that the two documents responsive to item #3 were exempt in their entirety. Tab F.

17. By letter 24 November 2009, Plaintiff appealed these two NSA determinations. Tab G. Plaintiff did not, however, challenge the sufficiency of NSA's search for records responsive to item #3 of Plaintiff's FOIA request. NSA placed Plaintiff's appeal in its appeal queue for processing. On 4 February 2010, before NSA

² These two documents were draft versions of NSA policies, and they were not finalized at the time the Agency conducted its search for records responsive to the Plaintiff's 25 June 2009 FOIA request. NSA has recently released the finalized versions of these two policies, NSA/CSS Policy 1-58 and IAD Management Directive 20, to the Plaintiff with redactions (pursuant to exemptions 1 and 3 of the FOIA) of classified information (for NSA/CSS Policy 1-58 only) and information protected from release by statute.

had processed Plaintiff's appeal, Plaintiff filed a civil action regarding its FOIA request to NSA. At that time, NSA ceased processing Plaintiff's appeal.

FOIA EXEMPTION ONE

18. Section 552(b)(1) of the FOIA provides that the FOIA does not require the release of matters that are specifically authorized - under criteria established by an Executive Order - to be kept secret in the interest of the national defense or foreign policy and are in fact properly classified pursuant to such Executive Order. The current Executive Order that establishes such criteria is E.O. 13526.

19. Section 1.4 of E.O. 13526 provides that information shall not be considered for classification unless it falls within one (or more) of eight specifically enumerated categories of information. The categories of classified information in the documents at issue here are those found in Section 1.4(b), which includes foreign government information; 1.4(c), which include intelligence activities (including covert action), intelligence sources and methods, or cryptology; and Section 1.4(g), which include vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security.

20. In my role as a TOP SECRET classification authority, I have reviewed the NSA information responsive to the Plaintiff's FOIA request to the NSA. For the following reasons, I have determined that certain information (marked with the (b)(1) exemption code) withheld in NSA/CSS Policy 1-58 is currently and properly classified at the SECRET level in accordance with E.O. 13526. Accordingly, the release of this information could reasonably be expected to cause serious damage to the national security.

21. The information in NSA/CSS Policy 1-58 that was withheld under Exemption 1, if released, would reveal operational details of NSA's implementation of the CNCI. The release of any of this information would reveal information about NSA's capabilities and limitations, and such a revelation could assist our adversaries in undermining NSA's cyberspace mission.

22. Further, any public disclosure of the details by which NSA leverages the capability of the agency to respond to cyber-threats (be they specific SIGINT or IAD capabilities), how NSA disseminates threat, vulnerability, mitigation and warning information, how NSA assists DHS in the performance of its cyber-mission, how NSA ensures the security of US government national security systems, and how NSA protects the security of our own systems would alert our adversaries to our capabilities in cyberspace. Revelation of this sort of information would reasonably be expected to cause our adversaries to change the methods that they use and thus thwart our efforts to identify vulnerabilities and mitigate them and to assist others with this task.

23. Thus, disclosing any operational or amplifying details of NSA's implementation of the CNCI, which is the information withheld by NSA in Policy 1-58, would provide our adversaries with critical information about the capabilities and limitations of NSA. Accordingly, any operational or amplifying details of NSA's implementation of the CNCI are exempt from disclosure, as indicated by the (b)(1) markings in NSA/CSS Policy 1-58, by Exemption 1 of the FOIA because the information is currently and properly classified in accordance with E.O. 13526.

FOIA EXEMPTION THREE

24. Section 552(b)(3) of the FOIA provides that the FOIA does not require the release of matters that are specifically exempted from disclosure by statute, provided that such statute requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or established particular criteria for withholding or refers to particular types of matter to be withheld. *See* 5 U.S.C. sec. 552(b)(3). Review of the application of Exemption 3 statutes consists solely of determining that the statute relied upon qualifies as an Exemption 3 statute and that the information withheld falls within the scope of the statute.

25. The information withheld from NSA/CSS Policy 1-58 and IAD Management Directive 20 falls squarely within the scope of several statutes. The first of these statutes is a statutory privilege unique to NSA. As set forth in section 6 of the National Security Agency Act of 1959, Public Law 86-36 (50 U.S.C. § 402 note) (“Section 6”), “[n]othing in this Act or any other law . . . shall be construed to require the disclosure of the organization or any function of the National Security Agency, [or] of any information with respect to the activities thereof. . . .” (Emphasis added). Congress, in enacting the language in this statute, decided that disclosure of any information relating to NSA activities is potentially harmful. Federal courts have held that the protection provided by this statutory privilege is, by its very terms, absolute. *See, e.g., Linder v. NSA*, 94 F. 3d 693 (D.C. Cir. 1996). Section 6 states unequivocally that, notwithstanding any other law, including the FOIA, NSA cannot be compelled to disclose any information with respect to its activities. *See Hayden*, 608 F.2d at 1389. Further, while in this case the harm would be serious, NSA is not required to demonstrate specific

harm to national security when invoking this statutory privilege, but only to show that the information relates to its activities. *Id.* at 1390. To invoke this privilege, NSA must demonstrate only that the information it seeks to protect falls within the scope of section 6. NSA's functions and activities are therefore protected from disclosure regardless of whether or not the information is classified.

26. The second applicable statute is 18 U.S.C. § 798. This statute prohibits the unauthorized disclosure of classified information: (i) concerning the communications intelligence activities of the United States; or (ii) obtained by the process of communication intelligence derived from the communications of any foreign government. The term "communications intelligence," as defined by 18 U.S.C. § 798(b), means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients.

27. The third applicable statute is Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. § 403-1(i)(1), which states that "[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure." NSA, as a member agency of the U.S. intelligence community, must also protect intelligence sources and methods. Like the protection afforded to core NSA activities by Section 6 of the NSA Act of 1959, the protection afforded to intelligence sources and methods is absolute. *See Central Intelligence Agency v. Sims*, 471 U.S. 159 (1985). Whether the sources and methods at issue are classified is irrelevant for purposes of the protection afforded by 50 U.S.C. § 403-1(i)(1). *Id.*

28. The information at issue here, i.e. how NSA implements the CNCI, falls squarely within the scope of all three above-cited Exemption 3 statutes. Information about NSA's implementation of the CNCI directly relates to one of the Agency's core functions and activities of its Information Assurance mission, which is to assist in the protection of U.S. information systems. Likewise, this information also directly relates to NSA's SIGINT mission, which is part of NSA's role in the CNCI. Thus, revealing any operational details on how NSA implements the CNCI, would directly reveal NSA's functions and activities, which are afforded absolute protection. Accordingly, all of the information withheld in NSA/CSS Policy 1-58 and IAD Management Directive 20 is exempt pursuant to Exemption 3 based on Section 6 alone.

29. Additionally, some of the same information that is exempt based on Section 6 is also exempt under Exemption 3 based on 18 U.S.C. § 798, because disclosure would reveal classified information derived from NSA's exploitation of foreign communications, and based on 50 U.S.C. § 403-1(i)(1), because the information concerns intelligence sources and methods.

NSPD 54

30. As discussed above, the Agency identified NSPD-54 as being a document responsive to item #1 of the Plaintiff's FOIA request. This document did not originate with NSA, but rather, it originated with the National Security Council (NSC) and Homeland Security Council (HSC).

31. NSPD 54 reflects – as its name indicates – direction from the President himself on sensitive and national security topics. NSPD 54 was issued by the President and included Presidential direction on specific actions to be undertaken by the federal

government to safeguard federal cybersecurity. This direction was issued to a number of high ranking Presidential advisers, Cabinet officials, and agency heads, including (*inter alia*) the Director of NSA.

32. NSPD 54 clearly reflected the President's concern with the confidentiality of the document. In a Memorandum accompanying NSPD 54 (dated 9 January 2008), the White House instructed all recipients of NSPD 54 to refer all public requests for disclosure of NSPD-54 to the NSC and HSC. The Memorandum makes explicitly clear that a recipient of NSPD 54 *should not* distribute or disclose the document without express permission from the White House.

33. Further, NSA is restricted in disseminating NSPD-54 even within the NSA; the Memorandum accompanying NSPD 54 forbids such intra-agency distribution except on a need to know basis. Explicit White House permission is further required before redistributing NSPD-54 to overseas organizations within the Agency or to other Governmental agencies/organizations.

34. Although this document can be withheld in its entirety based on Exemption 5 (presidential communication privilege), NSA has withheld one paragraph in this document which pertains to its activities based on Exemption 1 of the FOIA because the information is currently and properly classified in accordance with E.O. 13526 and Exemption 3 because the information is protected by statutes: Section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 402 note (Pub. L. 86-36) and Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004, 50 U.S.C. §403-1(i)(1).

**NSA'S DETERMINATION THAT IT COULD NOT LOCATE RECORDS
RESPONSIVE TO ITEM #2 OF PLAINTIFF'S FOIA REQUEST**

35. In item #2 of its FOIA request, Plaintiff sought “The full text, including unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation.” As stated above, the CNCI was implemented in NSPD-54, which is a White House privileged document. As such, any unreported sections of the CNCI, if they exist, would not be subject to the FOIA. Although, as noted herein, the NSA has a copy of NSPD 54 – and thus, has a copy of those sections of the NSPD 54 related to the CNCI – the “full text” of the CNCI is subject to withholding because the entire NSPD 54 document (including the sections related to the CNCI) is subject to withholding under the presidential communications privilege.

36. Likewise, regarding the Plaintiff’s request for “executing protocols” that were “distributed” to the agencies who have implemented the CNCI (item #2 in Plaintiff’s FOIA request), such “executing protocols,” if they exist, would be White House records, not NSA records. Further, a reasonable search uncovered no such documents in NSA’s possession when the NSA searched for responsive records by giving plain meaning to Plaintiff’s request and thus searched for “Executing protocols” that were “distributed to” to the NSA – meaning, protocols that emanated from outside the NSA and were “distributed to” NSA. The Agency conducted its searches in June and July 2009 within the relevant NSA organizations and including the Signal Intelligence Directorate and Information Assurance Directorate organizations. NSA concluded that any directives on how to execute the CNCI would have been received by the organizations who conducted

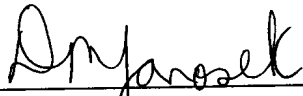
the search because they would be executing aspects of the CNCI. The search for records responsive to item #2 was conducted by the same organizations that searched for records responsive to item #3 of the Plaintiff's FOIA request, but none of them located any such "executing protocols" that were "distributed" to NSA except for NSPD 54, which was also responsive to item #1 of the Plaintiff's request.

37. Giving plain meaning to Plaintiff's request, the NSA's search that was conducted in June/July 2009 did not locate any protocols from outside the agency (other than NSPD 54 itself) directing the NSA as to how it was to implement NSPD 54, although these searches produced records responsive to item #3 of the Plaintiff's FOIA request. Accordingly, those organizations were asked to search all files for any documents that had been distributed to NSA on how to execute the CNCI. None of these organizations located any such responsive executing protocols.

38. Based on the above, it is my determination that NSA conducted a reasonable search but did not locate any records that were responsive to item #2 of the Plaintiff's FOIA request.

I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed this 11th day of October 2011 pursuant to 28 U.S.C. § 1746.



DIANE M. JANOSEK
Deputy Associate Director for Policy and Records
National Security Agency

DECLARATION OF MARY RONAN

I, Mary Ronan, hereby declare:

1. I am the Director of the Access Management Office for the National Security Staff (NSS), Washington, D.C. The NSS is a component of the Executive Office of the President (EOP). I have served in this position since 2006, when the Staff for the National Security Council (NSC) was known as the National Security Council Staff. Now the NSS encompasses the staff of both the NSC and the Homeland Security Council (HSC). Prior to my service at the White House complex, I held similar positions in the National Archives and Records Administration. In my current position, I have been delegated classification and declassification authority in accordance with the provisions of Executive Order 13526.

2. Among my duties as Director of Access Management for the NSS, I am responsible for handling document referrals from federal agencies seeking guidance as to whether NSS records in their custody may be released. In executing this function, I determine whether information that is requested from NSS records may be declassified consistent with Executive Order 13526, or whether it must remain classified to protect the national security interests of the United States. In consultation with counsel, I also help determine whether information that is

requested from NSS records is subject to a claim of privilege, and therefore whether its release would adversely affect important presidential interests.

3. Section 1.3(a) of Executive Order 13526 provides that the authority to classify information originally may be exercised only by the President and, in the performance of executive duties, the Vice President; agency heads and officials designated by the President in the Federal Register; and United States Government officials delegated this authority pursuant to section 1.3(c) of the Order. Section 1.3(c)(2) provides that TOP SECRET original classification authority may be delegated only by the President; in the performance of executive duties, the Vice President; or an agency head or official designated pursuant to section 1.3(a)(2) of the Order. Section 1.3(b) of the Executive Order provides that original TOP SECRET classification authority includes the authority to classify information originally as SECRET and CONFIDENTIAL. As an original classification authority, I am authorized to conduct classification reviews and to make original classification decisions.

4. I have reviewed and am generally familiar with the request for records made by Electronic Privacy Information Center ("EPIC") that is the subject of the litigation in EPIC v. National Security Agency, No. 10-00196 (BAH). The subject of

the EPIC request is (among other things) National Security Presidential Directive-54/Homeland Security Presidential Directive-23 ("NSPD-54").

5. The NSS is the original classification authority for NSPD-54. In March 2010, I completed an initial classification review of NSPD-54, made certain classification adjustments to a number of paragraphs, and ultimately determined that the document as a whole was properly classified as TOP SECRET, for reasons consistent with the rationale I describe below.

6. During the week of October 4, 2011, the NSS received a request to conduct another classification review of NSPD-54. Once again, I personally reviewed NSPD-54 in order to respond to the request.

7. NSPD-54 is a confidential communication from the President of the United States to a select and limited group of senior foreign policy advisors, cabinet officials, and agency heads on the subject of cybersecurity policy. The directive was originally accompanied by a transmittal memo from a Special Assistant to the President who was the HSC's Executive Secretary, which was distributed to all recipients. The memo emphasized NSPD-54's close-hold nature and the need to safeguard its content, a need that continues to this day. Specifically, the cover memo explained that NSPD-54 communicates presidential decisions and orders that require careful safeguarding. The

memo prohibited dissemination of the document beyond its authorized recipients without White House approval and further instructed that even within receiving agencies, copies should be distributed only on a need to know basis.

8. NSPD-54 as a whole is classified as TOP SECRET. Individual paragraphs within NSPD-54 have different classification markings ranging from UNCLASSIFIED to, SECRET, and TOP SECRET.

9. Title 5 U.S.C. Section 552(b)(1) states that FOIA does not apply to matters that are "(A) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy," and "(B) are in fact properly classified pursuant to such Executive order."

10. I have personally reviewed NSPD-54 and have concluded that the information marked classified in this document continues to meet the classification criteria of E.O. 13526 and should therefore be withheld pursuant to FOIA Exemption (b)(1).

11. I have determined that, as understood under E.O. 13526, the information in this document that has been classified as TOP SECRET constitutes information the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. I have also determined that, as understood under E.O. 13526, the

information in this document that has been classified as SECRET constitutes information the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. The information contained within NSPD 54 has been and remains properly classified under Sections 1.4(c), because it involves intelligence activities or intelligence sources and methods; 1.4(d), because it involves foreign relations or foreign activities of the United States; 1.4(e), because it concerns scientific, technological, or economic matters relating to the national security; and 1.4(g), because it involves vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security.

12. I have also determined that the information contained within NSPD-54 has not been classified in order to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interests of national security.

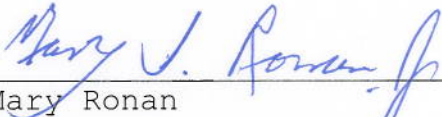
13. While it is possible to segregate parts of NSPD-54 that can be released consistent with FOIA exemption (b)(1) without adversely affecting the national security of the United States, NSPD-54 should be withheld in full under FOIA exemption

b(5). NSPD-54 is a confidential communication from the President of the United States to a select and limited group of senior foreign policy advisors, cabinet officials, and agency heads, including (*inter alia*) the Directors of NSA and the Office of Management and Budget, and the Secretaries of State, Defense, Homeland Security, and Treasury. The directive communicates presidential decisions and orders designed to improve the internal workings of the Executive Branch - specifically, a variety of actions designed to increase the security of federal cyber assets and improve the federal government's capacity to deter and respond to various threats to federal systems and information. Moreover, NSPD-54 solicits follow-up information from the same Departments and Agencies to the President, at least one purpose of which is to measure the efficacy of the President's chosen courses of action.

14. Disclosure of even the unclassified material contained in NSPD-54 would undermine the President's ability to communicate confidentially with his senior advisors, cabinet officials, and agency heads on sensitive matters that fall within his core constitutional duties - namely, the development of a coordinated strategy within the Executive Branch to protect the nation from cyber security risks. Disclosure would reveal the form and content of sensitive Presidential deliberations, thereby sacrificing the confidentiality necessary to ensure that

the President receives candid and timely advice. Moreover, disclosure would interfere with the President's ability to communicate his decisions confidentially, which would frustrate his ability to exercise control over the executive branch. More generally, disclosure of NSPD 54 would undermine the ability of federal officials to communicate effectively on efforts to promote cybsersecurity - a confidential process that the President deemed important to achieving the purposes of NSPD 54. Thus, disclosure of NSPD-54 would impede the President's ability to perform his constitutional duties.

Pursuant to 28 U.S.C. 1746, I declare under penalty of perjury that the foregoing is true and correct.



Mary Ronan
Director, Access Management
National Security Staff

Executed on: October 11, 2011.

TAB A

DOCID: 3574783

ELECTRONIC PRIVACY INFORMATION CENTER

1718 CONNECTICUT AVENUE NW, SUITE 200
WASHINGTON, D.C. 20009
202-483-1140
FAX 202-483-1248

CONFIDENTIAL - SUBJECT TO ATTORNEY-CLIENT PRIVILEGE
ANY DISSEMINATION, DISTRIBUTION, OR COPYING OF THIS COMMUNICATION BY OTHER THAN
ITS ADDRESSEE IS STRICTLY PROHIBITED. IF THIS FACSIMILE HAS BEEN RECEIVED IN ERROR,
PLEASE IMMEDIATELY NOTIFY THE SENDER

TO: FOIA/PA OFFICE

FROM: MARK PERRY

COMPANY:

DATE:

National Security Agency

6/25/2009

RECIPIENT'S FAX NUMBER:

SENDER'S EMAIL:

443.479.3612

perry@epic.org

RECIPIENT'S TELEPHONE NUMBER:

SENDER'S TELEPHONE NUMBER:

202.483.1140

TOTAL NO. OF PAGES INCLUDING COVER:

5

COMMENTS:



1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 463 1148 (tel)
+1 202 463 1248 (fax)
www.epic.org

June 25, 2009

VIA FACSIMILE (443.479.3612)

National Security Agency
Attn: FOIA/PA Office (DJP4)
9800 Savage Road, Suite 6248
Ft. George G. Meade, MD 200755-6248

RE: Freedom of Information Act Request and Request for Expedited Processing

Dear FOIA/PA Officer:

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC"). EPIC seeks National Security Presidential Directive 54 (the Directive) and related records in possession of the agency.

Background

In January 2008, George W. Bush issued the Directive, but it was never released to the public.¹ Under this secret Directive,² the Comprehensive National Cybersecurity Initiative (CNCI) was formed to "improve how the federal government protects sensitive information from hackers and nation states trying to break into agency networks."³ In February 2009, President Obama appointed Melissa Hathaway as the head of a 60-day review of government's cybersecurity efforts (the Hathaway Report).⁴ In April 2009, Senator Jay Rockefeller (D-WV)

¹ Jill R. Aitoro, *The Comprehensive National Cybersecurity Initiative*, NEXTGOV, June 1, 2009, http://www.nextgov.com/the_basics/tb_20090601_8569.php.

² "The CNCI – officially established in January when President Bush signed National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 – is a multi-agency, multi-year plan that lays out twelve steps to securing the federal government's cyber networks. DHS has been tasked to lead or play a major role in many of these tasks. This bold, much-needed approach to cybersecurity will lead to a fundamental shift in the way the Department approaches the security of U.S. networks." Letter from Joseph I. Lieberman, Chairman, and Susan M. Collins, Ranking Member, United States Senate Committee on Homeland Security and Governmental Affairs to Michael Chertoff, Secretary, Department of Homeland Security (May 1, 2008), available at http://hsgac.senate.gov/public/_files/5108LiebermanCollinslettertoChertoff.pdf.

³ *Id.*

⁴ Jaikumar Vijayan, *Obama Taps Bush Aide Melissa Hathaway to Review Federal Cybersecurity Efforts*, COMPUTER WORLD: SECURITY, Feb. 9, 2009, <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127682>.

DOCID: 3574783

introduced to Congress the Cybersecurity Act of 2009 (S. 773), still pending in the Senate Committee on Commerce, Science, and Transportation.⁵

The NSA has been involved with the development of cybersecurity policy since the Directive was issued.⁶ In fact, the Washington Post noted the NSA, along with FBI and CIA, as agencies charged with the responsibility of implementing the CNCI.⁷ The March 2009 resignation letter of the former head of the DHS National Cybersecurity Center, Rod Beckstrom, confirms that the NSA did in fact gain tremendous influence over DHS cybersecurity operations. In his letter, Mr. Beckstrom asserted that the "NSA effectively controls DHS cyber efforts through . . . technology insertions, and the proposed move of two organizations under DHS (the National Protection and Programs Directorate and the National Cybersecurity Center) to a Fort Meade NSA facility."⁸ Therefore, NSA likely has possession and control of the documents EPIC seeks in this request.

Though privacy is highlighted in the Hathway Report, such considerations are noticeably absent from any practical application of the Cybersecurity Act. As Senators Joseph Lieberman and Susan Collins noted in their May 1, 2008 letter to DHS Secretary Michael Chertoff, efforts to "downgrade the classification or declassify information regarding [CNCI] would . . . permit broader collaboration with the privacy sector and outside experts."⁹ President Obama's recent focus on Transparency, Participation, and Collaboration between the public and executive agencies further justifies a renewed effort to disclose such information to the public. Releasing the documents sought in this request would provide the opportunity for meaningful public participation in the development of new security measures that may have a significant impact on civil liberties, such as privacy.¹⁰ The Senate Committee on Homeland Security and Governmental Affairs recognizes that cybersecurity initiatives must include actions to "...reassure [the public] that efforts to secure cyber networks will be appropriately balanced with respect for privacy and civil liberties."¹¹ The government cannot meaningfully make such assurances without making public the foundational documents underpinning the CNCI.

⁵ Jennifer Granick, *Federal Authority Over the Internet? The Cybersecurity Act of 2009*, ELECTRONIC FRONTIER FOUNDATION, Apr. 10, 2009, <http://www EFF.org/deeplinks/2009/04/cybersecurity-act>.

⁶ Jill R. Aitoro, *The Comprehensive National Cybersecurity Initiative*, NEXTGOV, June 1, 2009, http://www.nextgov.com/the_basics/tb_20090601_8569.php.

⁷ Ellen Nakashima, *Bush Order Expands Network Monitoring*, THE WASHINGTON POST, Jan. 26, 2009, available at <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html?wpisrc=newsletter>

⁸ Letter from Rod Beckstrom, Director, National Cybersecurity Center to Janet Napolitano, Secretary, Department of Homeland Security (March 5, 2009), available at <http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf>.

⁹ *Supra* note 2.

¹⁰ Memoranda from Barack Obama, President of the United States, on Transparency and Open Government (January 21, 2009) available at http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/.

¹¹ *Supra* note 2.

DOCID: 3574783

Documents Requested

Although the Initiative has been the primary source of cybersecurity rules since 2008, neither the Initiative nor the authorizing Directive has been released in full.¹² Gregory Garcia (then DHS Assistant Secretary of Cybersecurity and Telecommunications) stated in February 2009 that “too much was kept secret.”¹³ The policy goals in the Directive, and the implementation of those goals in the Initiative, have directed virtually all cybersecurity regulation. Therefore, EPIC requests copies of the following agency records:

1. The text of the National Security Presidential Directive 54 otherwise referred to as The Homeland Security Presidential Directive 23.
2. The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation.
3. Any privacy policies related to either the Directive, the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative.

Request for Expedited Processing

This request warrants expedited processing because it is made by “a person primarily engaged in disseminating information . . .” and it pertains to a matter about which there is an “urgency to inform the public about an actual or alleged federal government activity.” 5 U.S.C. § 552(a)(6)(E)(v)(II).

EPIC is “primarily engaged in disseminating information.” *American Civil Liberties Union v. Department of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

Moreover, there is particular urgency for the public to obtain information about CNCI. The Cybersecurity Act of 2009 is presently under consideration by the Senate Committee on Commerce, Science, and Transportation. In order for meaningful public comment on this or subsequent cybersecurity measures, the public must be aware of current programs. Neither DHS nor NSA has provided information on measures adopted to safeguard the privacy of citizens’ personal information in connection to the directive or CNCI. The public should be informed of NSA’s ongoing role in CNCI.

Request for “News Media” Status

EPIC is a non-profit, educational organization that routinely and systematically disseminates information to the public. EPIC is a representative of the news media. *Epic v. Dep’t of Defense*, 241, F.Supp. 2d 5 (D.D.C. 2003).

¹² See, supra note 1.


¹³ *Id.*

DOCID: 3574783

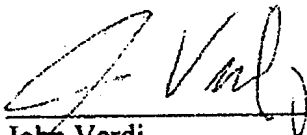
Based on our status as a "news media" requester, we are entitled to receive the requested records with only duplication fees assessed. Further, because disclosure of this information will "contribute significantly to public understanding of the operations or activities of the government," as described above, any duplication fees should be waived.

Thank you for your consideration of this request. As provided in 5 U.S.C. § 552(a)(6)(E)(ii)(I), I will anticipate your determination on our request for expedited processing within ten (10) calendar days.

Sincerely,



Mark Joseph Perry
EPIC Clerk



John Verdi
Director, EPIC Open Government Project

TAB B



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 58987
1 July 2009

Mr. Mark J. Perry
Electronic Privacy Information Center
1718 Connecticut Avenue NW
Suite 200
Washington, DC 20009

Dear Mr. Perry:

This is an initial response to your Freedom of Information Act (FOIA) request submitted via facsimile on 25 June 2009, which was received by this office on 26 June 2009, for copies of the following records:

1. "The text of the National Security Presidential Directive 54 otherwise referred to as The Homeland Security Presidential Directive 23.
2. The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation.
3. Any privacy policies related to either the Directive, the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative."

Your request has been assigned Case Number 58987. This letter indicates that we have begun to process your request. There is certain information relating to this processing about which the FOIA and applicable Department of Defense (DOD) and NSA/CSS regulations require we inform you. For purposes of this request and based on the information you provided in your letter, you are considered a representative of the media. Unless you qualify for a fee waiver or reduction, you must pay for duplication in excess of the first 100 pages. Your request for a waiver of fees has been granted.

Please be advised that a FOIA request may be expedited if the requester has made a statement certified by the requester to be true and correct to the best of his/her knowledge that a compelling need exists. Compelling need is defined as follows:

FOIA Case: 58987

1. The failure to obtain the records on an expedited basis could reasonably be expected to pose an imminent threat to the life or physical safety of an individual.


2. The information is urgently needed by an individual primarily engaged in disseminating information to inform the public about actual or alleged Federal Government activity. Urgent need means that the information has a particular value that will be lost if not disseminated quickly.

A request will also be handled expeditiously, upon receipt of a certified statement by the requester, if the substantial due process rights of the requester would be impaired by the failure to process the request immediately and the information sought is not otherwise available; there is a humanitarian need which will promote the welfare and interest of mankind; or other narrowly construed exceptional circumstances exist.

Your request for expedited treatment has been denied because it does not meet the FOIA's criteria for expedited treatment. We will process your request in our normal processing queue.

The Initial Denial Authority for NSA is the Deputy Associate Director for Policy and Records, Diane M. Janosek. If you disagree with the decision regarding denial of your expedite request, you may file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal must be postmarked no later than 60 calendar days after the date of the initial denial letter. The appeal shall be in writing addressed to the NSA/CSS FOIA Appeal Authority (DJP4), National Security Agency, 9800 Savage Road STE 6248, Fort George G. Meade, MD 20755-6248. The appeal shall reference the denial and shall contain, in sufficient detail and particularity, the grounds upon which you believe expeditious processing is warranted. The NSA/CSS Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent any unusual circumstances.

Sincerely,



PAMELA N. PHILLIPS
Chief
FOIA/PA Office

TAB C



July 30, 2009

1718 Connecticut Ave NW

Suite 200

Washington DC 20009

USA

+1 202 483 1140 [tel]

+1 202 483 1248 [fax]

www.epic.org

BY CERTIFIED MAIL

NSA/CSS FOIA Appeal Authority (DJP4)
National Security Agency
9800 Savage Road STE 6248
Ft. George G. Meade, MD 20755-6248

RE: Freedom of Information Act Appeal (FOIA Case 58987)

Dear FOIA Appeals Officer:

This letter constitutes an appeal under the Freedom of Information Act ("FOIA"), 5 U.S.C § 552, and is submitted to the National Security Agency ("NSA") by the Electronic Privacy Information Center ("EPIC").

On June 25, 2009, EPIC requested, *via* facsimile, documents regarding National Security Directive 54 (the "Directive") and the Comprehensive National Cybersecurity Initiative (the "Initiative"). Specifically, EPIC requested:

1. The text of the National Security Presidential Directive 54 otherwise referred to as Homeland Security Presidential Directive 23.
2. The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation.
3. Any privacy policies related to either the Directive or the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative.

See Appendix 1 ("EPIC's FOIA Request").

Factual Background

In January 2008, George W. Bush issued the Directive, but it was never released to the public.¹ Under this secret Directive,² the Comprehensive National Cybersecurity Initiative

¹ Jill R. Aitoro, *The Comprehensive National Cybersecurity Initiative*, NEXTGOV, June 1, 2009, http://www.nextgov.com/the_basics/tb_20090601_8569.php.

(CNCI) was formed to “improve how the federal government protects sensitive information from hackers and nation states trying to break into agency networks.”³ In February 2009, President Obama appointed Melissa Hathaway as the head of a 60-day review of government’s cybersecurity efforts (the Hathaway Report).⁴ In April 2009, Senator Jay Rockefeller (D-WV) introduced to Congress the Cybersecurity Act of 2009 (S. 773), still pending in the Senate Committee on Commerce, Science, and Transportation.⁵

The NSA has been involved with the development of cybersecurity policy since the Directive was issued.⁶ In fact, the Washington Post noted the NSA, along with FBI and CIA, as agencies charged with the responsibility of implementing the CNCI.⁷ The March 2009 resignation letter of the former head of the DHS National Cybersecurity Center, Rod Beckstrom, confirms that the NSA did in fact gain tremendous influence over DHS cybersecurity operations. In his letter, Mr. Beckstrom asserted that the “NSA effectively controls DHS cyber efforts through . . . technology insertions, and the proposed move of two organizations under DHS (the National Protection and Programs Directorate and the National Cybersecurity Center) to a Fort Meade NSA facility.”⁸ Therefore, NSA likely has possession and control of the documents EPIC seeks in this request.

Though privacy is highlighted in the Hathaway Report, such considerations are noticeably absent from any practical application of the Cybersecurity Act. As Senators Joseph Lieberman and Susan Collins noted in their May 1, 2008 letter to DHS Secretary Michael Chertoff, efforts to “downgrade the classification or declassify information regarding [CNCI] would . . . permit broader collaboration with the privacy sector and outside experts.”⁹ President Obama’s recent focus on Transparency, Participation, and Collaboration between the public and executive agencies further justifies a renewed effort to disclose such information to the public. Releasing the documents sought in this request would provide the opportunity for meaningful public participation in the development of new security measures that may have a significant impact on

² “The CNCI – officially established in January when President Bush signed National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 – is a multi-agency, multi-year plan that lays out twelve steps to securing the federal government’s cyber networks. DHS has been tasked to lead or play a major role in many of these tasks. This bold, much-needed approach to cybersecurity will lead to a fundamental shift in the way the Department approaches the security of U.S. networks.” Letter from Joseph I. Lieberman, Chairman, and Susan M. Collins, Ranking Member, United States Senate Committee on Homeland Security and Governmental Affairs to Michael Chertoff, Secretary, Department of Homeland Security (May 1, 2008), *available at* http://hsgac.senate.gov/public/_files/5108LiebermanCollinslettertoChertoff.pdf.

³ *Id.*

⁴ Jaikumar Vijayan, *Obama Taps Bush Aide Melissa Hathaway to Review Federal Cybersecurity Efforts*, COMPUTER WORLD: SECURITY, Feb. 9, 2009,

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127682>.

⁵ Jennifer Granick, *Federal Authority Over the Internet? The Cybersecurity Act of 2009*, ELECTRONIC FRONTIER FOUNDATION, Apr. 10, 2009, <http://www.eff.org/deeplinks/2009/04/cybersecurity-act>

⁶ Jill R. Aitoro, *The Comprehensive National Cybersecurity Initiative*, NEXTGOV, June 1, 2009, http://www.nextgov.com/the_basics/tb_20090601_8569.php.

⁷ Ellen Nakashima, *Bush Order Expands Network Monitoring*, THE WASHINGTON POST, Jan. 26, 2009, *available at* <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html?wpisrc=newsletter>

⁸ Letter from Rod Beckstrom, Director, National Cybersecurity Center to Janet Napolitano, Secretary, Department of Homeland Security (March 5, 2009), *available at*

<http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf>.

⁹ *Supra* note 2.

DOCID: 3595906

civil liberties, such as privacy.¹⁰ The Senate Committee on Homeland Security and Governmental Affairs recognizes that cybersecurity initiatives must include actions to "...reassure [the public] that efforts to secure cyber networks will be appropriately balanced with respect for privacy and civil liberties."¹¹ The government cannot meaningfully make such assurances without making public the foundational documents underpinning the CNCI.

Procedural Background

On June 29, 2009, EPIC transmitted EPIC's FOIA Request to the NSA. *See* Appendix 1.

On July 1, 2009, the NSA wrote to EPIC, acknowledged receipt of EPIC's FOIA Request and denied EPIC's request for expedited processing, but did not make any substantive determination regarding EPIC's FOIA request. *See* 5 U.S.C. § 552(a)(6); *see also* Appendix 2.

EPIC Appeals the NSA's Failure to Disclose Records

EPIC hereby appeals the NSA's failure to make a timely determination regarding EPIC's FOIA Request. An agency must make a determination regarding a FOIA request within twenty working days. 5 U.S.C. § 552(a)(6); *see also Wash Post v. Dep't of Homeland Sec.*, 459 F. Supp. 2d 61, 74 (D.D.C. 2006) (citing *Payne Enterprises v. U.S.*, 837 F.2d 486, 494 (D.C. Cir. 1998)) (stating "FOIA was created to foster public awareness, and failure to process FOIA requests in a timely fashion is 'tantamount to denial.'").

EPIC Appeals the NSA's Denial of Its Request for Expedited Processing

EPIC appeals NSA's refusal to grant expedited processing for its FOIA request. The request warrants expedited processing because it is made by "a person primarily engaged in disseminating information . . ." and it pertains to a matter about which there is an "urgency to inform the public about an actual or alleged federal government activity." 5 U.S.C. § 552(a)(6)(E)(v)(II).

EPIC is "primarily engaged in disseminating information." *American Civil Liberties Union v. Department of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

Moreover, there is particular urgency for the public to obtain information about the Initiative. The Cybersecurity Act of 2009 is presently under consideration by the Senate Committee on Commerce, Science, and Transportation (S. 773). In order for EPIC to make meaningful public comment on this or subsequent security measures, EPIC and the public must be aware of current programs. Neither NSA nor the NSA has provided information on measures adopted to safeguard the privacy of citizens' personal information in connection to the directive or CNCI. The public should be informed of NSA's ongoing role in the Initiative prior to passage of the Cybersecurity Act currently under consideration.

¹⁰ Memoranda from Barack Obama, President of the United States, on Transparency and Open Government (January 21, 2009) available at http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/.


¹¹ *Supra* note 2.

DOCID: 3595906

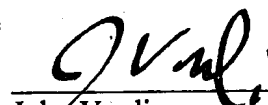
Conclusion

Thank you for prompt response to this appeal. As the FOIA provides, I anticipate that you will produce responsive documents within 10 working days. If you have any questions, please feel free to contact me or John Verdi at (202) 483-1140 or Verdi@epic.org.

Sincerely,



Mark Perry
EPIC Clerk



John Verdi
Director, EPIC Open Government Project

/enclosures

DOCID: 3595906

Appendix 1

EPIC's June 25, 2009 FOIA Request to the NSA

DOCID: 3595906

ELECTRONIC PRIVACY INFORMATION CENTER

1718 CONNECTICUT AVENUE NW, SUITE 200
WASHINGTON, D.C. 20009
202-483-1140
FAX 202-483-1248

CONFIDENTIAL -- SUBJECT TO ATTORNEY-CLIENT PRIVILEGE

ANY DISSEMINATION, DISTRIBUTION, OR COPYING OF THIS COMMUNICATION BY OTHER THAN
ITS ADDRESSEE IS STRICTLY PROHIBITED. IF THIS FACSIMILE HAS BEEN RECEIVED IN ERROR,
PLEASE IMMEDIATELY NOTIFY THE SENDER

TO: FOIA/PA OFFICE

FROM: MARK PERRY

COMPANY

DATE

National Security Agency

6/25/2009

RECIPIENT'S FAX NUMBER

SENDER'S EMAIL

443.479.3612

perry@epic.org

RECIPIENT'S TELEPHONE NUMBER

SENDER'S TELEPHONE NUMBER

202.483.1140

TOTAL NO. OF PAGES INCLUDING COVER:

5

COMMENTS:

DOCID: 3595906

introduced to Congress the Cybersecurity Act of 2009 (S. 773), still pending in the Senate Committee on Commerce, Science, and Transportation.⁵

The NSA has been involved with the development of cybersecurity policy since the Directive was issued.⁶ In fact, the Washington Post noted the NSA, along with FBI and CIA, as agencies charged with the responsibility of implementing the CNCI.⁷ The March 2009 resignation letter of the former head of the DHS National Cybersecurity Center, Rod Beckstrom, confirms that the NSA did in fact gain tremendous influence over DHS cybersecurity operations. In his letter, Mr. Beckstrom asserted that the “NSA effectively controls DHS cyber efforts through . . . technology insertions, and the proposed move of two organizations under DHS (the National Protection and Programs Directorate and the National Cybersecurity Center) to a Fort Meade NSA facility.”⁸ Therefore, NSA likely has possession and control of the documents EPIC seeks in this request.

Though privacy is highlighted in the Hathway Report, such considerations are noticeably absent from any practical application of the Cybersecurity Act. As Senators Joseph Lieberman and Susan Collins noted in their May 1, 2008 letter to DHS Secretary Michael Chertoff, efforts to “downgrade the classification or declassify information regarding [CNCI] would . . . permit broader collaboration with the privacy sector and outside experts.”⁹ President Obama’s recent focus on Transparency, Participation, and Collaboration between the public and executive agencies further justifies a renewed effort to disclose such information to the public. Releasing the documents sought in this request would provide the opportunity for meaningful public participation in the development of new security measures that may have a significant impact on civil liberties, such as privacy.¹⁰ The Senate Committee on Homeland Security and Governmental Affairs recognizes that cybersecurity initiatives must include actions to “...reassure [the public] that efforts to secure cyber networks will be appropriately balanced with respect for privacy and civil liberties.”¹¹ The government cannot meaningfully make such assurances without making public the foundational documents underpinning the CNCI.

⁵ Jennifer Granick, *Federal Authority Over the Internet? The Cybersecurity Act of 2009*, ELECTRONIC FRONTIER FOUNDATION, Apr 10, 2009, <http://www.eff.org/deeplinks/2009/04/cybersecurity-act>.

⁶ Jill R. Aitoro, *The Comprehensive National Cybersecurity Initiative*, NEXTGOV, June 1, 2009, http://www.nextgov.com/the_basics/tb_20090601_8569.php.

⁷ Ellen Nakashima, *Bush Order Expands Network Monitoring*, THE WASHINGTON POST, Jan 26, 2009, available at <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html?wpisrc=newsletter>

⁸ Letter from Rod Beckstrom, Director, National Cybersecurity Center to Janet Napolitano, Secretary, Department of Homeland Security (March 5, 2009), available at <http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf>

⁹ *Supra* note 2

¹⁰ Memoranda from Barack Obama, President of the United States, on Transparency and Open Government (January 21, 2009) available at http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/.

¹¹ *Supra* note 2

DOCID: 3595906

Documents Requested

Although the Initiative has been the primary source of cybersecurity rules since 2008, neither the Initiative nor the authorizing Directive has been released in full.¹² Gregory Garcia (then DHS Assistant Secretary of Cybersecurity and Telecommunications) stated in February 2009 that “too much was kept secret.”¹³ The policy goals in the Directive, and the implementation of those goals in the Initiative, have directed virtually all cybersecurity regulation. Therefore, EPIC requests copies of the following agency records:

1. The text of the National Security Presidential Directive 54 otherwise referred to as The Homeland Security Presidential Directive 23.
2. The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation.
3. Any privacy policies related to either the Directive, the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative.

Request for Expedited Processing

This request warrants expedited processing because it is made by “a person primarily engaged in disseminating information . . .” and it pertains to a matter about which there is an “urgency to inform the public about an actual or alleged federal government activity.” 5 U.S.C. § 552(a)(6)(E)(v)(II).

EPIC is “primarily engaged in disseminating information.” *American Civil Liberties Union v. Department of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

Moreover, there is particular urgency for the public to obtain information about CNCI. The Cybersecurity Act of 2009 is presently under consideration by the Senate Committee on Commerce, Science, and Transportation. In order for meaningful public comment on this or subsequent cybersecurity measures, the public must be aware of current programs. Neither DHS nor NSA has provided information on measures adopted to safeguard the privacy of citizens’ personal information in connection to the directive or CNCI. The public should be informed of NSA’s ongoing role in CNCI.

Request for “News Media” Status

EPIC is a non-profit, educational organization that routinely and systematically disseminates information to the public. EPIC is a representative of the news media. *Epic v. Dep’t of Defense*, 241, F.Supp. 2d 5 (D.D.C. 2003).

¹² See, supra note 1

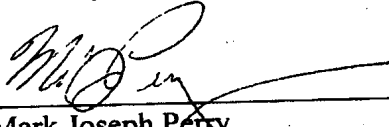
¹³ Id

DOCID: 3595906

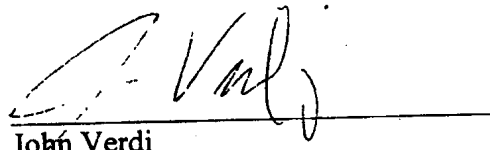
Based on our status as a "news media" requester, we are entitled to receive the requested records with only duplication fees assessed. Further, because disclosure of this information will "contribute significantly to public understanding of the operations or activities of the government," as described above, any duplication fees should be waived.

Thank you for your consideration of this request. As provided in 5 U.S.C. § 552(a)(6)(E)(ii)(I). I will anticipate your determination on our request for expedited processing within ten (10) calendar days.

Sincerely,



Mark Joseph Perry
EPIC Clerk



John Verdi
Director, EPIC Open Government Project

TIME : 06/25/2009 13:09
NAME : EPIC
FAX : 2024831248
TEL : 2024831140
SER.# : M7J214130

DATE, TIME	06/25 13:06
FAX NO./NAME	14434793612 ..
DURATION	00:02:35
PAGE(S)	05
RESULT	OK *
MODE	PHOTO
	ECM

* :COLOR FAX NOT AVAILABLE

DOCID: 3595906

Appendix 2

July 1, 2009 Letter from NSA to EPIC Confirming Receipt



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G MEADE, MARYLAND 20755-6000

FOIA Case: 58987
1 July 2009

Mr. Mark J. Perry
Electronic Privacy Information Center
1718 Connecticut Avenue NW
Suite 200
Washington, DC 20009

Dear Mr. Perry:

This is an initial response to your Freedom of Information Act (FOIA) request submitted via facsimile on 25 June 2009, which was received by this office on 26 June 2009, for copies of the following records:

1. "The text of the National Security Presidential Directive 54 otherwise referred to as The Homeland Security Presidential Directive 23.
2. The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation.
3. Any privacy policies related to either the Directive, the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative."

Your request has been assigned Case Number 58987. This letter indicates that we have begun to process your request. There is certain information relating to this processing about which the FOIA and applicable Department of Defense (DOD) and NSA/CSS regulations require we inform you. For purposes of this request and based on the information you provided in your letter, you are considered a representative of the media. Unless you qualify for a fee waiver or reduction, you must pay for duplication in excess of the first 100 pages. Your request for a waiver of fees has been granted.

Please be advised that a FOIA request may be expedited if the requester has made a statement certified by the requester to be true and correct to the best of his/her knowledge that a compelling need exists. Compelling need is defined as follows:

DOCID: 3595906

FOIA Case: 58987

1. The failure to obtain the records on an expedited basis could reasonably be expected to pose an imminent threat to the life or physical safety of an individual.

2. The information is urgently needed by an individual primarily engaged in disseminating information to inform the public about actual or alleged Federal Government activity. Urgent need means that the information has a particular value that will be lost if not disseminated quickly.

A request will also be handled expeditiously, upon receipt of a certified statement by the requester, if the substantial due process rights of the requester would be impaired by the failure to process the request immediately and the information sought is not otherwise available; there is a humanitarian need which will promote the welfare and interest of mankind; or other narrowly construed exceptional circumstances exist.

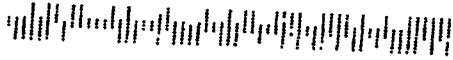
Your request for expedited treatment has been denied because it does not meet the FOIA's criteria for expedited treatment. We will process your request in our normal processing queue.

The Initial Denial Authority for NSA is the Deputy Associate Director for Policy and Records, Diane M. Janosek. If you disagree with the decision regarding denial of your expedite request, you may file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal must be postmarked no later than 60 calendar days after the date of the initial denial letter. The appeal shall be in writing addressed to the NSA/CSS FOIA Appeal Authority (DJP4), National Security Agency, 9800 Savage Road STE 6248, Fort George G. Meade, MD 20755-6248. The appeal shall reference the denial and shall contain, in sufficient detail and particularity, the grounds upon which you believe expeditious processing is warranted. The NSA/CSS Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent any unusual circumstances.

Sincerely,



PAMELA N. PHILLIPS
Chief
FOIA/PA Office



7006 2150 0001 7646 6922

PLACE STICKER AT TOP OF ENVELOPE TO THE RIGHT OF THE RETURN ADDRESS. FOLD AT DOTTED LINE.

CERTIFIED MAIL



7006 2150 0001 7646 6922

CONTROLLED MAIL



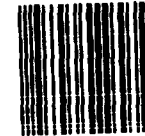
ELECTRONIC PRIVACY INFORMATION CENTER

epic.org

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA

OPEN BY PBGS
JUL 31 2009
INSPECTED BY PBGS

NSA/CSS FOIA Appeal Authority (DJP4)
National Security Agency
9800 Savage Road STE 6248
Ft. George G. Meade, MD 20755-6248



U.S. POSTAGE
PAID
WASHINGTON, DC
20009
JUL 30 '09
AMOUNT

\$4.02
00019074-05

1000

20755

TAB D



Case No. 58987/Appeal No. 3470

12 August 2009

Mr. Mark Perry
Electronic Privacy Information Center
1718 Connecticut Avenue, NW, Suite 200
Washington, DC 20009

Dear Mr. Perry:

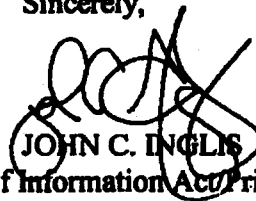
I am writing in response to your 30 July 2009 letter appealing the National Security Agency's (NSA) decision to deny your request for expedited processing of your Freedom of Information Act (FOIA) request. You had requested copies of the following records:

1. "The text of the National Security Presidential Directive 54 otherwise referred to as Homeland Security Presidential Directive 23.
2. The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation.
3. Any privacy policies related to either the Directive or the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative."

I have reviewed your original request, the Chief of the FOIA/PA Office's response to you, and your appeal letter. As a result of my review, I have decided to grant your request for expedited processing based on the information you provided on appeal.

Your case has been returned to the FOIA Office for expedited processing. If you have any questions, please contact the FOIA Office on 301-688-6527 and refer to Case Number 58987.

Sincerely,



JOHN C. INGLIS

Freedom of Information Act/Privacy Act
Appeals Authority

TAB E



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 58987A
14 August 2009

Mr. Mark J. Perry
Electronic Privacy Information Center
1718 Connecticut Avenue NW
Suite 200
Washington, DC 20009

Dear Mr. Perry:

This further responds to your Freedom of Information Act (FOIA) request submitted via the Internet on 25 June 2009, which was received by this office on 26 June 2009, for copies of the following records:

1. "The text of the National Security Presidential Directive 54 otherwise referred to as The Homeland Security Presidential Directive 23.
2. The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation, and
3. Any privacy policies related to either the Directive, the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative."

As previously provided, your request has been assigned Case Number 58987.

As you are aware from our Appeal Authority letter dated 13 August 2009, your appeal for expedited processing has been granted.

We have completed our search for records responsive to your request. Two of the documents responsive to request item #3 have been previously released under the FOIA and are enclosed with this response. If you would like a current review of these documents to ascertain if further information is releasable, please notify our office. Certain information has been deleted from the enclosures.

FOIA Case: 58987A

The information deleted from the documents was found to be currently and properly classified in accordance with Executive Order 12958, as amended. This information meets the criteria for classification as set forth in Subparagraphs (c) of Section 1.4 and remains SECRET as provided in Section 1.2 of the Executive Order. The information is classified because its disclosure could reasonably be expected to cause serious damage to the national security. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)).

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in these documents. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 403-1(i); and Section 6, Public Law 86-36 (50 U.S. Code 402 note).

The Initial Denial Authority for NSA information is the Deputy Associate Director for Policy and Records, Diane M. Janosek. Since the deletions from the enclosures may be construed as a partial denial of your request, you are hereby advised of this Agency's appeal procedures. Any person denied access to information may file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal must be postmarked no later than 60 calendar days from the date of the initial denial letter. The appeal shall be in writing addressed to the NSA/CSS FOIA Appeal Authority (DJ4), National Security Agency, 9800 Savage Road STE 6248, Fort George G. Meade, MD 20755-6248. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes release of the information is required. The NSA/CSS Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent any unusual circumstances.

Since your request has been expedited, the remaining material responsive has been assigned for review to determine releasability and will be completed as expeditiously as possible.

Correspondence related to your request should include the case number assigned to your request, which is included in the first paragraph of this letter. Your letter should be addressed to National Security Agency, FOIA Office (DJP4), 9800 Savage Road STE 6248, Ft. George G. Meade, MD 20755-6248 or may be sent by facsimile to 443-479-3612. If sent by fax, it should be marked

for the attention of the FOIA office. The telephone number of the FOIA office is 301-688-6527.

Sincerely,

A handwritten signature in black ink, appearing to read "Pamela N. Phillips", enclosed within a rectangular border.

PAMELA N. PHILLIPS
Chief
FOIA/PA Office

Encls:
a/s

TAB F



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 58987B
26 October 2009

Mr. Mark J. Perry
Electronic Privacy Information Center
1718 Connecticut Avenue NW
Suite 200
Washington, DC 20009

Dear Mr. Perry:

This further responds to your Freedom of Information Act (FOIA) request submitted via the Internet on 25 June 2009, which was received by this office on 26 June 2009, for copies of the following records:

1. "The text of the National Security Presidential Directive 54 otherwise referred to as The Homeland Security Presidential Directive 23;
2. The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation; and
3. Any privacy policies related to either the Directive, the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative."

As you recall, we provided you with two documents responsive to item 3 of your request on 14 August 2009 (copy enclosed). Your request has been further processed under the provisions of the FOIA. A thorough search of our files was conducted, but no records responsive to item 2 of your request were located. Three documents (26 pages) responsive to items 1 and 3 of your request have been reviewed by this Agency as required by the FOIA.

Two documents responsive to item 3 have been withheld in their entirety. Both documents are exempt from release pursuant to the fifth exemption of the FOIA. This exemption applies to inter-agency or intra-agency memoranda or letters which would not be available by law to a party in litigation with the agency, protecting information that is normally privileged in the civil discovery context, such as information that is part of a predecisional deliberative process.

Some of the information in one of the documents was also found to be currently and properly classified in accordance with Executive Order 12958, as amended. This information meets the criteria for classification as set forth in Subparagraph (c) of

Section 1.4 and remains classified SECRET and CONFIDENTIAL as provided in Section 1.2 of the Executive Order. The information is classified because its disclosure could reasonably be expected to cause serious damage to the national security. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)).

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in both withheld documents. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 403-1(i); and Section 6, Public Law 86-36 (50 U.S. Code 402 note).

The Initial Denial Authority for NSA information is the Deputy Associate Director for Policy and Records, Diane M. Janosek. Because we were unable to locate records responsive to item 2 of your request and because two documents were withheld in their entirety, you may consider this to be a partial denial of your request. You are hereby advised of this Agency's appeal procedures. Any person notified of an adverse determination may file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal must be postmarked no later than 60 calendar days after the date of the initial denial. The appeal shall be in writing addressed to the NSA/CSS FOIA Appeal Authority (DJP4), National Security Agency, 9800 Savage Road STE 6248, Fort George G. Meade, MD 20755-6248. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes release of the information is required. The NSA/CSS FOIA Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent any unusual circumstances.

Please be advised that the record responsive to item 1 of your request did not originate with this Agency. Because we are unable to make determinations as to the releasability of information other than our own, the subject document has been referred to the National Security Council for review and direct response to you.

Sincerely,



PAMELA N. PHILLIPS
Chief
FOIA/PA Office

Encl:
a/s

TAB G

DOCID: 3635254

ELECTRONIC PRIVACY INFORMATION CENTER
REF ID: A3635254



November 24, 2009

BY CERTIFIED MAIL
NSA/CSS FOIA Appeal Authority (DJP4)
National Security Agency
9800 Savage Road STE 6248
Ft. George G. Meade, MD 20755-6248

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 (tel)
+1 202 483 1248 (fax)
www.epic.org

RE: Freedom of Information Act Appeal (FOIA Case 58987)

Dear FOIA Appeals Officer:

This letter constitutes an appeal under the Freedom of Information Act (“FOIA”), 5 USC § 552, and is submitted to the National Security Agency (“NSA”) by the Electronic Privacy information Center (“EPIC”).

On June 25, 2009, EPIC requested agency records regarding National Security Presidential Directive 54 (the “Directive”) and the Comprehensive National Cybersecurity Initiative (the “Initiative”). Specifically, EPIC requested the following:

1. The text of National Security Presidential Directive 54, otherwise referred to as Homeland Security Presidential Directive 23.
2. The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation.
3. Any privacy policies related to either the Directive or the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative.

Factual Background

The documents sought are clearly in possession of the agency. In January 2008, George W. Bush issued the Directive, but it was never released to the public.¹ Under this secret Directive,² the Comprehensive National Cybersecurity Initiative (CNCI) was

¹ Jill R. Aitoro, *The Comprehensive National Cybersecurity Initiative*, NEXTGOV, June 1, 2009, http://www.nextgov.com/the_basics/tb_20090601_8569.php.

² “The CNCI – officially established in January when President Bush signed National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 – is a multi-agency, multi-year plan that lays out twelve steps to securing the federal government’s cyber networks. DHS has been tasked to lead or play a major role in many of these tasks. This bold, much-needed approach to cybersecurity will lead to a fundamental shift in the way the Department approaches the security of U.S. networks.” Letter from Joseph

formed to “improve how the federal government protects sensitive information from hackers and nation states trying to break into agency networks.”³ In February 2009, President Obama appointed Melissa Hathaway as the head of a 60-day review of government’s cybersecurity efforts (the “Hathaway Report”).⁴ In April 2009, Senator Jay Rockefeller (D-WV) introduced to Congress the Cybersecurity Act of 2009 (S. 773), still pending in the Senate Committee on Commerce, Science, and Transportation.⁵

Since the Directive was issued, the NSA has pursued policies set out in the still-secret document.⁶ In fact, the Washington Post noted the NSA, along with FBI and CIA, as agencies charged with the responsibility of implementing the CNCI.⁷ The March 2009 resignation letter of the former head of the DHS National Cybersecurity Center, Rod Beckstrom, confirms that the NSA did in fact gain tremendous influence over DHS cybersecurity operations. In his letter, Mr. Beckstrom asserted that the “NSA effectively controls DHS cyber efforts through . . . technology insertions, and the proposed move of two organizations under DHS (the National Protection and Programs Directorate and the National Cybersecurity Center) to a Fort Meade NSA facility.”⁸

Though privacy is highlighted in the Hathaway Report, such considerations are noticeably absent from any practical application of the Cybersecurity Act. As Senators Joseph Lieberman and Susan Collins noted in their May 1, 2008 letter to DHS Secretary Michael Chertoff, efforts to “downgrade the classification or declassify information regarding [CNCI] would . . . permit broader collaboration with the privacy sector and outside experts.”⁹ President Obama’s recent focus on Transparency, Participation, and Collaboration between the public and executive agencies further justifies a renewed effort to disclose such information to the public. Releasing the documents sought in this request would provide the opportunity for meaningful public participation in the development of new security measures that may have a significant impact on civil liberties, such as

I. Lieberman, Chairman, and Susan M. Collins, Ranking Member, United States Senate Committee on Homeland Security and Governmental Affairs to Michael Chertoff, Secretary, Department of Homeland Security (May 1, 2008), *available at* http://hsgac.senate.gov/public/_files/5108LiebermanCollinslettertoChertoff.pdf.

³ *Id.*

⁴ Jaikumar Vijayan, *Obama Taps Bush Aide Melissa Hathaway to Review Federal Cybersecurity Efforts*, COMPUTER WORLD: SECURITY, Feb. 9, 2009, <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127682>.

⁵ Thomas, S.773 Bill Summary, *available at* <http://thomas.loc.gov/cgi-bin/bdquery/z?d111:s.00773>; see also Jennifer Granick, *Federal Authority Over the Internet? The Cybersecurity Act of 2009*, ELECTRONIC FRONTIER FOUNDATION, Apr. 10, 2009, <http://www EFF.org/deeplinks/2009/04/cybersecurity-act>.

⁶ Jill R. Aitoro, *The Comprehensive National Cybersecurity Initiative*, NEXTGOV, June 1, 2009, http://www.nextgov.com/the_basics/tb_20090601_8569.php.

⁷ Ellen Nakashima, *Bush Order Expands Network Monitoring*, THE WASHINGTON POST, Jan. 26, 2009, *available at* <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html?wpisrc=newsletter>

⁸ Letter from Rod Beckstrom, Director, National Cybersecurity Center to Janet Napolitano, Secretary, Department of Homeland Security (March 5, 2009), *available at* <http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf>.

⁹ Letter from Lieberman & Collins, *supra* note 2.

privacy.¹⁰ The Senate Committee on Homeland Security and Governmental Affairs recognizes that cybersecurity initiatives must include actions to "...reassure [the public] that efforts to secure cyber networks will be appropriately balanced with respect for privacy and civil liberties."¹¹

Taken together, these developments underscore the important public interest in making available to the public the Directive that undergirds the government's policy on cyber security. Without this disclosure, as sought by EPIC in this matter, the government cannot meaningfully make assurances about the adequacy of privacy and civil liberties safeguards.

Procedural Background

On June 29, 2009, EPIC transmitted EPIC's FOIA request to the NSA. *See* Appendix 1 ("EPIC's FOIA request").

On July 1, 2009, the NSA wrote to EPIC, acknowledged receipt of EPIC's FOIA request, but denied EPIC's request for expedited processing and did not make any substantive determination regarding EPIC's FOIA request. *See* 5 U.S.C. § 552(a)(6); *see also* Appendix 2.

On July 30, 2009, EPIC transmitted a written administrative appeal by certified mail to the NSA. *See* Appendix 3. EPIC appealed the NSA's failure to make a timely substantive determination regarding its request as required under 5 U.S.C. § 552(a)(6), as well as the NSA's denial of EPIC's request for expedited processing.

In a letter dated August 12, 2009, the NSA replied to EPIC's appeal of July 30. *See* Appendix 4. In this response, the NSA FOIA Appeals Authority granted the request for expedited processing, but made no substantive determination regarding EPIC's FOIA request.

In a subsequent letter, dated August 14, 2009, the NSA acknowledged the grant of expedited processing and stated that it had completed its search for responsive records. *See* Appendix 5. This letter further stated that two documents responsive to part 3 of EPIC's FOIA request¹² had been released previously under the FOIA in partially redacted form, and these two documents were enclosed with the letter. With respect to other documents identified by the agency, this letter stated only that "the remaining material responsive has been assigned for review to determine releasability and will be completed as expeditiously as possible."

In a letter dated October 26, 2009, the NSA responded with substantive determinations regarding that remaining material. *See* Appendix 6. This letter stated that

¹⁰ Memoranda from Barack Obama, President of the United States, on Transparency and Open Government (January 21, 2009) available at http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/.

¹¹ Letter from Lieberman & Collins, *supra* note 2.

¹² Appendix 1 at 3 ("Any privacy policies related to either the Directive or the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative.").

the NSA identified one document responsive to part 1 of EPIC's FOIA request,¹³ zero documents as responsive to part 2 of EPIC's FOIA request,¹⁴ and two additional documents as responsive to part 3 of EPIC's FOIA request.¹⁵

With respect to the document identified as responsive to part 1 of EPIC's FOIA request (the text of National Security Presidential Directive 54), the NSA refused to disclose the document. Instead, the NSA stated that because the record "did not originate with" the NSA, the document "has been referred to the National Security Council for review and direct response to" EPIC. The NSA withheld the documents responsive to part 3 of EPIC's FOIA request in full, allegedly pursuant to FOIA Exemption b(5). The NSA also stated that portions of the responsive documents were exempt from disclosure pursuant to Exemptions b(1) and b(3).

EPIC Appeals the NSA's Failure to Disclose Records

Request Part 1: EPIC hereby appeals the NSA's failure to disclose the record identified as responsive to part 1 of EPIC's FOIA request—the document is presumably NSPD 54. The FOIA does not define the term "agency records," but the NSA's published rules defines such records as:

The products of data compilation . . . made or received by an agency of the United States Government under Federal law in connection with the transaction of public business and in NSA/CSS's possession and control at the time the FOIA request is made.

32 C.F.R. § 299.2(c)(1). This definition is consistent with the standard established by the Supreme Court in *Dep't of Justice v. Tax Analysts*, 492 U.S. 136 (1989).

In its letter to EPIC dated October 26, 2009, the NSA admitted that the Directive is in its possession and control. That the NSA received the Directive in connection with the transaction of public business is well established above. The NSA's sole justification for refusing to disclose the Directive is that the record "did not originate" with the agency.

Although the agency cited no authority in the October 26 letter for the decision to refer the request to the National Security Council, presumably the NSA took the action pursuant to the relevant agency regulation, which reads:

Records or portions thereof originated by other agencies or information of primary interest to other agencies found in NSA/CSS records shall be handled as follows:

- (1) The originating agency's FOIA Authority shall be provided with a copy of the request and the stated records.

¹³ Appendix 1 at 3 ("The text of National Security Presidential Directive 54, otherwise referred to as Homeland Security Presidential Directive 23.")

¹⁴ Appendix 1 at 3 ("The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation.")

¹⁵ *supra* note 12.

- (2) The requester shall be advised of the referral, except when notification would reveal exempt information.

32 C.F.R. § 299.5(k). This regulation does not apply here, however, because the National Security Council is not an “agency” under the FOIA. *Armstrong v. Executive Office of the President*, 90 F.3d 553 (D.C. Cir. 1996). As such, the Directive is not a record originated by another agency, under the meaning of the applicable regulation. Additionally, the National Security Council has no designated FOIA Authority, making compliance with this regulation impossible in this case.

Even if it did apply here, the regulation itself is overbroad with no justification in the statute. The FOIA makes no provision for referring requests to outside entities. Instead it allows for a showing of “unusual circumstances” and includes in that definition “the need for consultation, which shall be conducted with all practicable speed, with another agency having a substantial interest in the determination of the request.” 5 U.S.C. § 552(a)(6)(B)(iii). The D.C. Circuit has held that “when an agency receives a FOIA request for ‘agency records’ in its possession it must take responsibility for processing the request. *It cannot simply refuse to act on the ground that the documents originated elsewhere.*” *McGehee v. CIA*, 697 F.2d 1095, 1110 (D.C. Cir. 1983), *vacated in part and aff’d in part*, 712 F.2d 1076 (D.C. Cir. 1983) (emphasis added). The D.C. Circuit held that forwarding requests to another body constitutes improper withholding “if its net effect is significantly to impair the requester’s ability to obtain the records or significantly to increase the amount of time he must wait to obtain them” and the agency fails to make “a showing that the procedure significantly improves the quality of the process.” *Id.*¹⁶

McGehee is only the first in a line of cases upholding the principle that unjustified referral to another entity in place of response constitutes improper withholding agency records. The D.C. Circuit repeated and clarified the rule in a second case almost immediately. *Paisley v. CIA*, 712 F.2d 686, 691 (D.C. Cir. 1983), *vacated in part*, 724 F.2d 201 (D.C. Cir. 1984). In that case, the court found that documents in possession of the FBI and CIA were agency records and subject to the FOIA even though they had originated in Congress or the Department of Justice. *Id.* In *Peralta v. U.S. Attorney’s Office*, 136 F.3d 169 (D.C. Cir. 1998), the Executive Office for U.S. Attorneys had forwarded the plaintiff’s FOIA request to the FBI and the district court had ruled that this satisfied its obligations. Even though the U.S. Attorneys and the FBI are both components of the Department of Justice, the D.C. Circuit reversed and ordered the district court to consider the referral question in light of *McGehee* on remand. *Id.* at 175. The rule is so well-established in the D.C. Circuit that it has even been used as the basis for vacating an order with a simple per curiam opinion, as in *Williams v. FBI*, 1993 U.S. App. Lexis 16937 (D.C. Cir. 1993) (per curiam).

The Seventh Circuit has also adopted the rule and applied it to a U.S. Attorney’s office in *In re Wade*, 969 F.2d 241, 247–248 (7th Cir. 1993), holding, “Once a FOIA request has been made to an agency, that agency’s referral to a different agency regarding

¹⁶ The court also noted that a procedure “that resulted in very long delays would be highly difficult to justify.” *Id.* While it is possible that the National Security Council may choose to abide by the spirit of the FOIA and release the record, this particular referral’s effects will likely result in a much worse result: complete non-response.

disclosure does not divest the original agency of responsibility to respond to the FOIA request.” The D.C. District Court acknowledged that the McGehee rule “is well-settled in our circuit,” before ruling that “even though Customs referred [agency records] to other agencies for review and processing, Customs is still responsible for explaining their non-production.” *Greenberg v. U.S. Dep’t of Treasury*, 10 F. Supp. 2d 3, 18 (D.D.C. 1998). In one recent case in the D.C. District, the referral was to a United States probation office, which, like the National Security Council, is not an agency subject to the FOIA. *Maydak v. U.S. Dep’t of Justice*, 254 F. Supp. 2d 23. Although the district court in that case gave the agency the opportunity to supplement the record on this point, the court acknowledged that the plaintiff raised “a genuine legal issue about the propriety” of the referral, and stated that compelling release of the documents “may ultimately be an appropriate remedy.” *Id.* at 40.

The NSA’s failure to disclose the Directive is contrary to federal statute and controlling legal authority. The agency has based its action on a misapplication of its own regulation. EPIC appeals the NSA’s improper withholding of NSPD 54 and urges the agency to disclose the record in its possession as required by the Freedom of Information Act. 5 U.S.C. 552(a)(3)(A).

Request Part 2: EPIC hereby appeals the NSA’s failure to disclose any records responsive to part 2 of EPIC’s FOIA request. The October 26 letter from the Agency states only that no responsive records were located, in spite of a “thorough search.”

Agencies must conduct a search that is “reasonably calculated to uncover all relevant documents.” *Weisberg v. Dep’t of Justice*, 705 F.2d 1344, 1351 (D.C. Cir. 1983); *see also McGehee*, 697 F.2d at 1100 (D.C. Cir. 1983). “If challenged, [the agency] must demonstrate beyond material doubt that the search was reasonable.” *Kowalczyk v. Dep’t of Justice*, 73 F.3d 386, 388 (D.C. Cir. 1996) (quoting *Truitt v. Department of State*, 283 U.S. App. D.C. 86, 897 F.2d 540, 542 (D.C. Cir. 1990)). “The adequacy of the [agency’s] search, in turn, is judged by a standard of reasonableness and depends, not surprisingly, upon the facts of each case.” *Natural Res. Def. Council v. Dep’t of Def.*, 388 F. Supp. 2d 1086, 1095 (C.D. Cal. 2005) (quoting *Weisberg v. Dep’t of Justice*, 745 F.2d 1476, 1485 (D.C. Cir. 1984)). When an agency is unable to locate responsive documents, it bears the burden proving that its less than comprehensive search is reasonable under the circumstances. *McGehee*, 697 F.2d at 1101.

The Lieberman & Collins letter discussed above and cited in EPIC’s original FIOA request clearly states that the CNCI is a very large program involving the participation of multiple agencies over several years. The Washington Post has identified the NSA as one of the primary agencies responsible for its implementation, and its participation is also referred to in Mr. Beckstrom’s resignation letter. *See supra* notes 6–8 and accompanying text.

Given the NSA’s well-established responsibilities with respect to the Comprehensive National Cybersecurity Initiative, it is very unlikely that a truly “thorough search” by the NSA would fail to turn up a single record satisfying request part 2 – “The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation.”

Request Part 3: EPIC hereby appeals the NSA's failure to disclose the two records identified by the Agency in the October 26 letter as responsive to part 3 of EPIC's FOIA request. The NSA alleges that both documents are exempt in full pursuant to FOIA Exemption b(5), that portions of one document are partially exempt pursuant to Exemption b(1), and that portions of both documents are exempt pursuant to Exemption b(3).

The NSA's full withholding under FOIA Exemption b(5) was improper. That exemption permits an agency to withhold records that constitute "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency." 5 U.S.C. § 522(b)(5). As acknowledged by the NSA in its explanation for the withholding, this exemption protects "information that is normally privileged in the civil discovery context, such as information that is part of a predecisional deliberative process." This phrasing by the Agency suggests that these two documents qualify for the deliberative process privilege as recognized by the Supreme Court in *NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 150–54 (1975). Yet records responsive to part 3 of EPIC's FOIA request would not be properly withheld under this privilege.

When describing this privilege, the Supreme Court specifically differentiated between predecisional documents and post-decisional documents, only finding protection for the former. *Id.* at 151–53. Additionally, the Court has cited the affirmative disclosure requirements of subsection (a)(2) of the FOIA—including "statements of policy and interpretations which have been adopted by the agency"—as evidence of "a strong congressional aversion to secret agency law." *Id.* at 153 (internal citation omitted). Part 3 of EPIC's request was for "privacy policies . . . including but not limited to contracts or other documents describing privacy policies for information shared with private contractors." EPIC did not request draft version of privacy policies, which might qualify as "predecisional." Rather, EPIC's FOIA request specifies final privacy policies. Records responsive to this request almost certainly constitute statements of agency policy, rather than predecisional deliberative documents. As such, the NSA's assertion of Exemption b(5) to withhold these documents is improper. Additionally, to the extent that any of the documents are actually contracts with private enterprises, those records may not be withheld pursuant to Exemption b(5) because voluntary disclosure to non-agency third parties generally constitutes waiver of the exemption. *Chilivis v. SEC*, 673 F.2d 1205, 1212 (11th Cir. 1982); *Cooper v. Dep't of Navy*, 594 F.2d 484, 486 (5th Cir. 1979).

EPIC also appeals the bases asserted for partially withholding the two records that the NSA has identified as responsive to part 3 of EPIC's FOIA request. In its letter, the NSA described parts of one record as "currently and properly classified in accordance with Executive Order 12958, as amended," and therefore exempt from disclosure under 5 U.S.C. § 522(b)(1). Additionally, NSA asserts Exemption b(3) as to portions of both records, and alleges that the information is exempt pursuant to various statutes. The Agency has not established any factual basis for these withholdings. Because the documents were withheld in full pursuant to Exemption b(5), it is impossible for EPIC to determine whether these asserted exemptions are proper without additional information concerning the records.

DOCID: 3635254

REF ID: A3635254

Conclusion

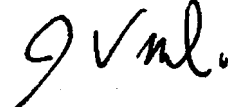
By improperly referring a request to an outside entity instead of disclosing an agency record in its possession and control, the NSA has failed to comply with the FOIA. The Agency also failed to comply by performing an inadequate search for responsive documents and by asserting inapplicable exemptions in order to improperly withhold other documents. The NSA's improper withholding of these records also flatly contravenes a recent memorandum on the Freedom of Information Act issued by the President of the United States and explicit FOIA guidance promulgated by the Attorney General. On January 21, 2009, President Obama stated that "The Freedom of Information Act should be administered with a clear presumption: In the face of doubt, openness prevails. . . . The presumption of disclosure should be applied to all decisions involving FOIA."¹⁷ On March 19, 2009, Attorney General Eric Holder promulgated new FOIA guidelines for heads of all Executive Departments and Agencies to ensure that the "nation's fundamental commitment to open government . . . is realized in practice."¹⁸

EPIC appeals the NSA's failure to disclose responsive documents and its failure to perform an adequate, reasonable search for the agency records described in EPIC's FOIA request. EPIC reiterates its request for expedited processing in this appeal—a request the NSA granted as to EPIC's FOIA request.

Sincerely,



Jared Kaprove
EPIC Domestic Surveillance Counsel



John Verdi
Director, EPIC Open Government Project

/enclosures

¹⁷ President Barack Obama, "Memorandum for the Heads of Executive Departments and Agencies, Subject: Freedom of Information Act," January 21, 2009, available at <http://www.justice.gov/ag/foia-memo-march2009.pdf>

¹⁸ Available at <http://www.justice.gov/ag/foia-memo-march2009.pdf>

DOCID: 3635254

REF ID: A3635254

Appendix 1

EPIC's June 25, 2009 FOIA request to the NSA



1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
www.epic.org

June 25, 2009

VIA FACSIMILE (443.479.3612)

National Security Agency
Attn: FOIA/PA Office (DJP4)
9800 Savage Road, Suite 6248
Ft. George G. Meade, MD 200755-6248

RE: Freedom of Information Act Request and Request for Expedited Processing

Dear FOIA/PA Officer:

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC"). EPIC seeks National Security Presidential Directive 54 (the Directive) and related records in possession of the agency.

Background

In January 2008, George W. Bush issued the Directive, but it was never released to the public.¹ Under this secret Directive,² the Comprehensive National Cybersecurity Initiative (CNCI) was formed to "improve how the federal government protects sensitive information from hackers and nation states trying to break into agency networks."³ In February 2009, President Obama appointed Melissa Hathaway as the head of a 60-day review of government's cybersecurity efforts (the Hathaway Report).⁴ In April 2009, Senator Jay Rockefeller (D-WV)

¹ Jill R. Aitoro, *The Comprehensive National Cybersecurity Initiative*, NEXTGOV, June 1, 2009, http://www.nextgov.com/the_basics/tb_20090601_8569.php.

² "The CNCI – officially established in January when President Bush signed National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 – is a multi-agency, multi-year plan that lays out twelve steps to securing the federal government's cyber networks. DHS has been tasked to lead or play a major role in many of these tasks. This bold, much-needed approach to cybersecurity will lead to a fundamental shift in the way the Department approaches the security of U.S. networks." Letter from Joseph I. Lieberman, Chairman, and Susan M. Collins, Ranking Member, United States Senate Committee on Homeland Security and Governmental Affairs to Michael Chertoff, Secretary, Department of Homeland Security (May 1, 2008), *available at* http://hsgac.senate.gov/public/_files/5108LiebermanCollinslettertoChertoff.pdf.

³ *Id.*

⁴ Jaikumar Vijayan, *Obama Taps Bush Aide Melissa Hathaway to Review Federal Cybersecurity Efforts*, COMPUTER WORLD: SECURITY, Feb. 9, 2009, <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127682>.

DOCID: 3635254

REF ID: A3635254

introduced to Congress the Cybersecurity Act of 2009 (S. 773), still pending in the Senate Committee on Commerce, Science, and Transportation.⁵

The NSA has been involved with the development of cybersecurity policy since the Directive was issued.⁶ In fact, the Washington Post noted the NSA, along with FBI and CIA, as agencies charged with the responsibility of implementing the CNCI.⁷ The March 2009 resignation letter of the former head of the DHS National Cybersecurity Center, Rod Beckstrom, confirms that the NSA did in fact gain tremendous influence over DHS cybersecurity operations. In his letter, Mr. Beckstrom asserted that the “NSA effectively controls DHS cyber efforts through . . . technology insertions, and the proposed move of two organizations under DHS (the National Protection and Programs Directorate and the National Cybersecurity Center) to a Fort Meade NSA facility.”⁸ Therefore, NSA likely has possession and control of the documents EPIC seeks in this request.

Though privacy is highlighted in the Hathway Report, such considerations are noticeably absent from any practical application of the Cybersecurity Act. As Senators Joseph Lieberman and Susan Collins noted in their May 1, 2008 letter to DHS Secretary Michael Chertoff, efforts to “downgrade the classification or declassify information regarding [CNCI] would . . . permit broader collaboration with the privacy sector and outside experts.”⁹ President Obama’s recent focus on Transparency, Participation, and Collaboration between the public and executive agencies further justifies a renewed effort to disclose such information to the public. Releasing the documents sought in this request would provide the opportunity for meaningful public participation in the development of new security measures that may have a significant impact on civil liberties, such as privacy.¹⁰ The Senate Committee on Homeland Security and Governmental Affairs recognizes that cybersecurity initiatives must include actions to “...reassure [the public] that efforts to secure cyber networks will be appropriately balanced with respect for privacy and civil liberties.”¹¹ The government cannot meaningfully make such assurances without making public the foundational documents underpinning the CNCI.

⁵ Jennifer Granick, *Federal Authority Over the Internet? The Cybersecurity Act of 2009*, ELECTRONIC FRONTIER FOUNDATION, Apr. 10, 2009, <http://www.eff.org/deeplinks/2009/04/cybersecurity-act>.

⁶ Jill R. Aitoro, *The Comprehensive National Cybersecurity Initiative*, NEXTGOV, June 1, 2009, http://www.nextgov.com/the_basics/tb_20090601_8569.php.

⁷ Ellen Nakashima, *Bush Order Expands Network Monitoring*, THE WASHINGTON POST, Jan. 26, 2009, available at <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html?wpisrc=newsletter>

⁸ Letter from Rod Beckstrom, Director, National Cybersecurity Center to Janet Napolitano, Secretary, Department of Homeland Security (March 5, 2009), available at <http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf>.

⁹ *Supra* note 2.

¹⁰ Memoranda from Barack Obama, President of the United States, on Transparency and Open Government (January 21, 2009) available at http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/.

¹¹ *Supra* note 2.

DOCID: 3635254

REF ID: A3635254

Documents Requested

Although the Initiative has been the primary source of cybersecurity rules since 2008, neither the Initiative nor the authorizing Directive has been released in full.¹² Gregory Garcia (then DHS Assistant Secretary of Cybersecurity and Telecommunications) stated in February 2009 that “too much was kept secret.”¹³ The policy goals in the Directive, and the implementation of those goals in the Initiative, have directed virtually all cybersecurity regulation. Therefore, EPIC requests copies of the following agency records:

1. The text of the National Security Presidential Directive 54 otherwise referred to as The Homeland Security Presidential Directive 23.
2. The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation.
3. Any privacy policies related to either the Directive, the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative.

Request for Expedited Processing

This request warrants expedited processing because it is made by “a person primarily engaged in disseminating information . . .” and it pertains to a matter about which there is an “urgency to inform the public about an actual or alleged federal government activity.” 5 U.S.C. § 552(a)(6)(E)(v)(II).

EPIC is “primarily engaged in disseminating information.” *American Civil Liberties Union v. Department of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

Moreover, there is particular urgency for the public to obtain information about CNCI. The Cybersecurity Act of 2009 is presently under consideration by the Senate Committee on Commerce, Science, and Transportation. In order for meaningful public comment on this or subsequent cybersecurity measures, the public must be aware of current programs. Neither DHS nor NSA has provided information on measures adopted to safeguard the privacy of citizens’ personal information in connection to the directive or CNCI. The public should be informed of NSA’s ongoing role in CNCI.

Request for “News Media” Status

EPIC is a non-profit, educational organization that routinely and systematically disseminates information to the public. EPIC is a representative of the news media. *Epic v. Dep’t of Defense*, 241, F.Supp. 2d 5 (D.D.C. 2003).

¹² See, *supra* note 1.

¹³ *Id.*

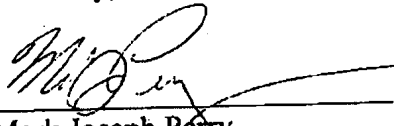
DOCID: 3635254

REF ID: A3635254

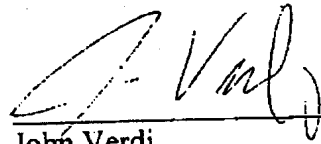
Based on our status as a "news media" requester, we are entitled to receive the requested records with only duplication fees assessed. Further, because disclosure of this information will "contribute significantly to public understanding of the operations or activities of the government," as described above, any duplication fees should be waived.

Thank you for your consideration of this request. As provided in 5 U.S.C. § 552(a)(6)(E)(ii)(I). I will anticipate your determination on our request for expedited processing within ten (10) calendar days.

Sincerely,



Mark Joseph Perry
EPIC Clerk



John Verdi
Director, EPIC Open Government Project

DOCID: 3635254

REF ID: A3635254

TRANSMISSION VERIFICATION REPORT

TIME : 06/25/2009 13:09
NAME : EPIC
FAX : 2024831248
TEL : 2024831140
SER.# : M7J214130

DATE, TIME	06/25 13:06
FAX NO./NAME	14434793612
DURATION	00:02:35
PAGE(S)	05
RESULT	OK *
MODE	PHOTO ECM

* :COLOR FAX NOT AVAILABLE

DOCID: 3635254

REF ID: A3635254

Appendix 2

NSA's July 1, 2009 initial response to EPIC

DOCID: 3635254

REF ID: A3635254



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 58987
1 July 2009

Mr. Mark J. Perry
Electronic Privacy Information Center
1718 Connecticut Avenue NW
Suite 200
Washington, DC 20009

Dear Mr. Perry:

This is an initial response to your Freedom of Information Act (FOIA) request submitted via facsimile on 25 June 2009, which was received by this office on 26 June 2009, for copies of the following records:

1. "The text of the National Security Presidential Directive 54 otherwise referred to as The Homeland Security Presidential Directive 23.
2. The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation.
3. Any privacy policies related to either the Directive, the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative."

Your request has been assigned Case Number 58987. This letter indicates that we have begun to process your request. There is certain information relating to this processing about which the FOIA and applicable Department of Defense (DOD) and NSA/CSS regulations require we inform you. For purposes of this request and based on the information you provided in your letter, you are considered a representative of the media. Unless you qualify for a fee waiver or reduction, you must pay for duplication in excess of the first 100 pages. Your request for a waiver of fees has been granted.

Please be advised that a FOIA request may be expedited if the requester has made a statement certified by the requester to be true and correct to the best of his/her knowledge that a compelling need exists. Compelling need is defined as follows:

DOCID: 3635254

REF ID: A3635254

FOIA Case: 58987

1. The failure to obtain the records on an expedited basis could reasonably be expected to pose an imminent threat to the life or physical safety of an individual.

2. The information is urgently needed by an individual primarily engaged in disseminating information to inform the public about actual or alleged Federal Government activity. Urgent need means that the information has a particular value that will be lost if not disseminated quickly.

A request will also be handled expeditiously, upon receipt of a certified statement by the requester, if the substantial due process rights of the requester would be impaired by the failure to process the request immediately and the information sought is not otherwise available; there is a humanitarian need which will promote the welfare and interest of mankind; or other narrowly construed exceptional circumstances exist.

Your request for expedited treatment has been denied because it does not meet the FOIA's criteria for expedited treatment. We will process your request in our normal processing queue.

The Initial Denial Authority for NSA is the Deputy Associate Director for Policy and Records, Diane M. Janosek. If you disagree with the decision regarding denial of your expedite request, you may file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal must be postmarked no later than 60 calendar days after the date of the initial denial letter. The appeal shall be in writing addressed to the NSA/CSS FOIA Appeal Authority (DJP4), National Security Agency, 9800 Savage Road STE 6248, Fort George G. Meade, MD 20755-6248. The appeal shall reference the denial and shall contain, in sufficient detail and particularity, the grounds upon which you believe expeditious processing is warranted. The NSA/CSS Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent any unusual circumstances.

Sincerely,



PAMELA N. PHILLIPS
Chief
FOIA/PA Office

DOCID: 3635254

REF ID: A3635254

Appendix 3

EPIC's July 30, 2009 administrative appeal to the NSA

DOCID: 3635254

REF ID: A3635254



July 30, 2009

1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA
+1 202 483 1140 (tel)
+1 202 483 1248 (fax)
www.epic.org

BY CERTIFIED MAIL

NSA/CSS FOIA Appeal Authority (DJP4)
National Security Agency
9800 Savage Road STE 6248
Ft. George G. Meade, MD 20755-6248

RE: Freedom of Information Act Appeal (FOIA Case 58987)

Dear FOIA Appeals Officer:

This letter constitutes an appeal under the Freedom of Information Act ("FOIA"), 5 U.S.C § 552, and is submitted to the National Security Agency ("NSA") by the Electronic Privacy Information Center ("EPIC").

On June 25, 2009, EPIC requested, *via* facsimile, documents regarding National Security Directive 54 (the "Directive") and the Comprehensive National Cybersecurity Initiative (the "Initiative"). Specifically, EPIC requested:

1. The text of the National Security Presidential Directive 54 otherwise referred to as Homeland Security Presidential Directive 23.
2. The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation.
3. Any privacy policies related to either the Directive or the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative.

See Appendix 1 ("EPIC's FOIA Request").

Factual Background

In January 2008, George W. Bush issued the Directive, but it was never released to the public.¹ Under this secret Directive,² the Comprehensive National Cybersecurity Initiative

¹ Jill R. Aitoro, *The Comprehensive National Cybersecurity Initiative*, NEXTGOV, June 1, 2009, http://www.nextgov.com/the_basics/tb_20090601_8569.php.

(CNCI) was formed to “improve how the federal government protects sensitive information from hackers and nation states trying to break into agency networks.”³ In February 2009, President Obama appointed Melissa Hathaway as the head of a 60-day review of government’s cybersecurity efforts (the Hathaway Report).⁴ In April 2009, Senator Jay Rockefeller (D-WV) introduced to Congress the Cybersecurity Act of 2009 (S. 773), still pending in the Senate Committee on Commerce, Science, and Transportation.⁵

The NSA has been involved with the development of cybersecurity policy since the Directive was issued.⁶ In fact, the Washington Post noted the NSA, along with FBI and CIA, as agencies charged with the responsibility of implementing the CNCI.⁷ The March 2009 resignation letter of the former head of the DHS National Cybersecurity Center, Rod Beckstrom, confirms that the NSA did in fact gain tremendous influence over DHS cybersecurity operations. In his letter, Mr. Beckstrom asserted that the “NSA effectively controls DHS cyber efforts through . . . technology insertions, and the proposed move of two organizations under DHS (the National Protection and Programs Directorate and the National Cybersecurity Center) to a Fort Meade NSA facility.”⁸ Therefore, NSA likely has possession and control of the documents EPIC seeks in this request.

Though privacy is highlighted in the Hathaway Report, such considerations are noticeably absent from any practical application of the Cybersecurity Act. As Senators Joseph Lieberman and Susan Collins noted in their May 1, 2008 letter to DHS Secretary Michael Chertoff, efforts to “downgrade the classification or declassify information regarding [CNCI] would . . . permit broader collaboration with the privacy sector and outside experts.”⁹ President Obama’s recent focus on Transparency, Participation, and Collaboration between the public and executive agencies further justifies a renewed effort to disclose such information to the public. Releasing the documents sought in this request would provide the opportunity for meaningful public participation in the development of new security measures that may have a significant impact on

² “The CNCI – officially established in January when President Bush signed National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 – is a multi-agency, multi-year plan that lays out twelve steps to securing the federal government’s cyber networks. DHS has been tasked to lead or play a major role in many of these tasks. This bold, much-needed approach to cybersecurity will lead to a fundamental shift in the way the Department approaches the security of U.S. networks.” Letter from Joseph I. Lieberman, Chairman, and Susan M. Collins, Ranking Member, United States Senate Committee on Homeland Security and Governmental Affairs to Michael Chertoff, Secretary, Department of Homeland Security (May 1, 2008), *available at* http://hsgac.senate.gov/public/_files/5108LiebermanCollinslettertoChertoff.pdf.

³ *Id.*

⁴ Jaikumar Vijayan, *Obama Taps Bush Aide Melissa Hathaway to Review Federal Cybersecurity Efforts*, COMPUTER WORLD: SECURITY, Feb. 9, 2009, <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127682>.

⁵ Jennifer Granick, *Federal Authority Over the Internet? The Cybersecurity Act of 2009*, ELECTRONIC FRONTIER FOUNDATION, Apr. 10, 2009, <http://www.eff.org/deeplinks/2009/04/cybersecurity-act>.

⁶ Jill R. Aitoro, *The Comprehensive National Cybersecurity Initiative*, NEXTGOV, June 1, 2009, http://www.nextgov.com/the_basics/tb_20090601_8569.php.

⁷ Ellen Nakashima, *Bush Order Expands Network Monitoring*, THE WASHINGTON POST, Jan. 26, 2009, *available at* <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html?wpisrc=newslctter>

⁸ Letter from Rod Beckstrom, Director, National Cybersecurity Center to Janet Napolitano, Secretary, Department of Homeland Security (March 5, 2009), *available at*

<http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf>.

⁹ *Supra* note 2.

DOCID: 3635254

REF ID: A3635254

civil liberties, such as privacy.¹⁰ The Senate Committee on Homeland Security and Governmental Affairs recognizes that cybersecurity initiatives must include actions to "...reassure [the public] that efforts to secure cyber networks will be appropriately balanced with respect for privacy and civil liberties."¹¹ The government cannot meaningfully make such assurances without making public the foundational documents underpinning the CNCI.

Procedural Background

On June 29, 2009, EPIC transmitted EPIC's FOIA Request to the NSA. *See* Appendix 1.

On July 1, 2009, the NSA wrote to EPIC, acknowledged receipt of EPIC's FOIA Request and denied EPIC's request for expedited processing, but did not make any substantive determination regarding EPIC's FOIA request. *See* 5 U.S.C. § 552(a)(6); *see also* Appendix 2.

EPIC Appeals the NSA's Failure to Disclose Records

EPIC hereby appeals the NSA's failure to make a timely determination regarding EPIC's FOIA Request. An agency must make a determination regarding a FOIA request within twenty working days. 5 U.S.C. § 522(a)(6); *see also Wash. Post v. Dep't of Homeland Sec.*, 459 F. Supp. 2d 61, 74 (D.D.C. 2006) (citing *Payne Enterprises v. U.S.*, 837 F.2d 486, 494 (D.C. Cir. 1998)) (stating "FOIA was created to foster public awareness, and failure to process FOIA requests in a timely fashion is 'tantamount to denial.'").

EPIC Appeals the NSA's Denial of Its Request for Expedited Processing

EPIC appeals NSA's refusal to grant expedited processing for its FOIA request. The request warrants expedited processing because it is made by "a person primarily engaged in disseminating information . . ." and it pertains to a matter about which there is an "urgency to inform the public about an actual or alleged federal government activity." 5 U.S.C. § 552(a)(6)(E)(v)(II).

EPIC is "primarily engaged in disseminating information." *American Civil Liberties Union v. Department of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

Moreover, there is particular urgency for the public to obtain information about the Initiative. The Cybersecurity Act of 2009 is presently under consideration by the Senate Committee on Commerce, Science, and Transportation (S. 773). In order for EPIC to make meaningful public comment on this or subsequent security measures, EPIC and the public must be aware of current programs. Neither NSA nor the NSA has provided information on measures adopted to safeguard the privacy of citizens' personal information in connection to the directive or CNCI. The public should be informed of NSA's ongoing role in the Initiative prior to passage of the Cybersecurity Act currently under consideration.

¹⁰ Memoranda from Barack Obama, President of the United States, on Transparency and Open Government (January 21, 2009) available at http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/.

¹¹ *Supra* note 2.

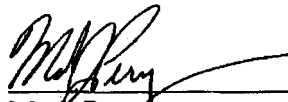
DOCID: 3635254

REF ID: A3635254


Conclusion

Thank you for prompt response to this appeal. As the FOIA provides, I anticipate that you will produce responsive documents within 10 working days. If you have any questions, please feel free to contact me or John Verdi at (202) 483-1140 or Verdi@epic.org.

Sincerely,



Mark Perry
EPIC Clerk



John Verdi
Director, EPIC Open Government Project

/enclosures

DOCID: 3635254

REF ID: A3635254

Appendix 4

NSA appeals authority August 12, 2009
letter to EPIC granting expedited processing

DOCID: 3635254

REF ID: A3635254



NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND 20755-6000

Case No. 58987/Appeal No. 3470
12 August 2009

Mr. Mark Perry
Electronic Privacy Information Center
1718 Connecticut Avenue, NW, Suite 200
Washington, DC 20009

Dear Mr. Perry:

I am writing in response to your 30 July 2009 letter appealing the National Security Agency's (NSA) decision to deny your request for expedited processing of your Freedom of Information Act (FOIA) request. You had requested copies of the following records:

1. "The text of the National Security Presidential Directive 54 otherwise referred to as Homeland Security Presidential Directive 23.
2. The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation.
3. Any privacy policies related to either the Directive or the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative."

I have reviewed your original request, the Chief of the FOIA/PA Office's response to you, and your appeal letter. As a result of my review, I have decided to grant your request for expedited processing based on the information you provided on appeal.

Your case has been returned to the FOIA Office for expedited processing. If you have any questions, please contact the FOIA Office on 301-688-6527 and refer to Case Number 58987.

Sincerely,

A handwritten signature in black ink, appearing to read "John C. Inglis".

JOHN C. INGLIS
Freedom of Information Act/Privacy Act
Appeals Authority

DOCID: 3635254

REF ID: A3635254

Appendix 5

NSA's August 14, 2009 letter to EPIC

DOCID: 3635254

REF ID: A3635254



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 58987A
14 August 2009

Mr. Mark J. Perry
Electronic Privacy Information Center
1718 Connecticut Avenue NW
Suite 200
Washington, DC 20009

Dear Mr. Perry:

This further responds to your Freedom of Information Act (FOIA) request submitted via the Internet on 25 June 2009, which was received by this office on 26 June 2009, for copies of the following records:

1. "The text of the National Security Presidential Directive 54 otherwise referred to as The Homeland Security Presidential Directive 23.
2. The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation, and
3. Any privacy policies related to either the Directive, the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative."

As previously provided, your request has been assigned Case Number 58987.

As you are aware from our Appeal Authority letter dated 13 August 2009, your appeal for expedited processing has been granted.

We have completed our search for records responsive to your request. Two of the documents responsive to request item #3 have been previously released under the FOIA and are enclosed with this response. If you would like a current review of these documents to ascertain if further information is

releasable, please notify our office. Certain information has been deleted from the enclosures.

The information deleted from the documents was found to be currently and properly classified in accordance with Executive Order 12958, as amended. This information meets the criteria for classification as set forth in Subparagraphs (c) of Section 1.4 and remains SECRET as provided in Section 1.2 of the Executive Order. The information is classified because its disclosure could reasonably be expected to cause serious damage to the national security. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)).

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in these documents. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 403-1(i); and Section 6, Public Law 86-36 (50 U.S. Code 402 note).

The Initial Denial Authority for NSA information is the Deputy Associate Director for Policy and Records, Diane M. Janosek. Since the deletions from the enclosures may be construed as a partial denial of your request, you are hereby advised of this Agency's appeal procedures. Any person denied access to information may file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal must be postmarked no later than 60 calendar days from the date of the initial denial letter. The appeal shall be in writing addressed to the NSA/CSS FOIA Appeal Authority (DJ4), National Security Agency, 9800 Savage Road STE 6248, Fort George G. Meade, MD 20755-6248. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes release of the information is required. The NSA/CSS Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent any unusual circumstances.

Since your request has been expedited, the remaining material responsive has been assigned for review to determine releasability and will be completed as expeditiously as possible.

Correspondence related to your request should include the case number assigned to your request, which is included in the first paragraph of this letter. Your letter should be addressed to National Security Agency, FOIA Office

DOCID: 3635254

REF ID: A3635254

Appendix 6

NSA's October 26 letter to EPIC



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 58987B
26 October 2009

Mr. Mark J. Perry
Electronic Privacy Information Center
1718 Connecticut Avenue NW
Suite 200
Washington, DC 20009

Dear Mr. Perry:

This further responds to your Freedom of Information Act (FOIA) request submitted via the Internet on 25 June 2009, which was received by this office on 26 June 2009, for copies of the following records:

1. "The text of the National Security Presidential Directive 54 otherwise referred to as The Homeland Security Presidential Directive 23;
2. The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementation; and
3. Any privacy policies related to either the Directive, the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative."

As you recall, we provided you with two documents responsive to item 3 of your request on 14 August 2009 (copy enclosed). Your request has been further processed under the provisions of the FOIA. A thorough search of our files was conducted, but no records responsive to item 2 of your request were located. Three documents (26 pages) responsive to items 1 and 3 of your request have been reviewed by this Agency as required by the FOIA.

Two documents responsive to item 3 have been withheld in their entirety. Both documents are exempt from release pursuant to the fifth exemption of the FOIA. This exemption applies to inter-agency or intra-agency memoranda or letters which would not be available by law to a party in litigation with the agency, protecting information that is normally privileged in the civil discovery context, such as information that is part of a predecisional deliberative process.

Some of the information in one of the documents was also found to be currently and properly classified in accordance with Executive Order 12958, as amended. This information meets the criteria for classification as set forth in Subparagraph (c) of Section 1.4 and remains classified SECRET and CONFIDENTIAL

REF ID: A3635254

DOCID: 3635254

FOIA Case: 58987B

as provided in Section 1.2 of the Executive Order. The information is classified because its disclosure could reasonably be expected to cause serious damage to the national security. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)).

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in both withheld documents. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 403-1(i); and Section 6, Public Law 86-36 (50 U.S. Code 402 note).

The Initial Denial Authority for NSA information is the Deputy Associate Director for Policy and Records, Diane M. Janosek. Because we were unable to locate records responsive to item 2 of your request and because two documents were withheld in their entirety, you may consider this to be a partial denial of your request. You are hereby advised of this Agency's appeal procedures. Any person notified of an adverse determination may file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal must be postmarked no later than 60 calendar days after the date of the initial denial. The appeal shall be in writing addressed to the NSA/CSS FOIA Appeal Authority (DJP4), National Security Agency, 9800 Savage Road STE 6248, Fort George G. Meade, MD 20755-6248. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes release of the information is required. The NSA/CSS FOIA Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent any unusual circumstances.

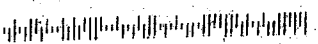
Please be advised that the record responsive to item 1 of your request did not originate with this Agency. Because we are unable to make determinations as to the releasability of information other than our own, the subject document has been referred to the National Security Council for review and direct response to you.

Sincerely,



PAMELA N. PHILLIPS
Chief
FOIA/PA Office

Encl:
a/s



7006 2150 0001 7646 7042



1000

20755

U.S. POST
PAID
WASHINGTON, DC 20009
NOV 24 2011
AMOUNT

\$45
000770E

ELECTRONIC PRIVACY INFORMATION CENTER

epic.org

1710 Connecticut Ave NW
Suite 200
Washington DC 20009
USA

FOIA Administrative Appeal
NSA/CSS FOIA Appeal Authority
(DJP4)
National Security Agency
9800 Savage Road STE 6248
Ft. George G. Meade, MD 20755-
6248

OPEN BY GCSI
NOV 29 2011
NSA/CSS FOIA APPEAL

1 - 1
CONTROLLED MAIL
 6248

7006 2350 0001 7646 7042

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

_____)	
ELECTRONIC PRIVACY)	
INFORMATION CENTER)	
)	
Plaintiff,)	
)	
v.)	Case No. 1:10-cv-00196-BAH
)	
NATIONAL SECURITY AGENCY)	
)	
)	
)	
Defendant.)	
_____)	

DEFENDANT’S STATEMENT OF MATERIAL FACTS NOT IN DISPUTE

Pursuant to Local Civil Rule 7(h) of the Rules of the United States District Court for the District of Columbia, defendant United States Department of State hereby submits the following statement of material facts not in dispute in connection with its motion for summary judgment under Rule 56(b) of the Federal Rules of Civil Procedure.

1. Plaintiff filed a FOIA request on June 25, 2009, which was received by the National Security Agency (“NSA”) on June 26, 2009, seeking information on the following: (1) The text of the National Security Presidential Directive 54 otherwise referred to as The Homeland Security Presidential Directive 23; (2) The full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to agencies in charge of its implementation; and (3) Any privacy policies related to the either the Directive, the Initiative, including but not limited to, contracts or other documents describing privacy

policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative. Declaration of Diane M. Janosek (“Janosek Decl.”) ¶ 10.

2. In this request, the Plaintiff also sought expedited processing and “news media” status. Janosek Decl. ¶ 10.

3. By letter dated July 1, 2009, the Chief, FOIA/PA Office, NSA/CSS, responded to Plaintiff’s FOIA request. In this initial response, NSA informed Plaintiff that its request for a waiver of fees was granted. NSA also informed Plaintiff that its request for expedited treatment was denied and that NSA would process the Plaintiff’s request in NSA’s normal processing queue. The NSA informed Plaintiff of its right to appeal the denial of Plaintiff’s request for expedited processing. Janosek Decl. ¶ 11.

4. By letter dated July 30, 2009, Plaintiff appealed NSA’s decision to deny it expedited processing. Janosek Decl. ¶ 12.

5. By letter dated August 12, 2009, NSA’s FOIA/PA Appeals Authority granted Plaintiff’s request for expedited processing based on his review of Plaintiff’s original request, the FOIA/PA Office’s initial response, and the information provided by Plaintiff on appeal. Janosek Decl. ¶ 12. Accordingly, Plaintiff’s FOIA request was placed in NSA’s expedite queue.

6. By letter dated August 14, 2009, the NSA FOIA Office informed the Plaintiff that its request was placed in the expedited queue and that NSA had finished its search for records responsive to its request. Janosek Decl. ¶ 13. NSA’s FOIA Office informed Plaintiff that two documents which were responsive to item 3 of its request had

been previously released under the FOIA with redactions and that NSA was providing these documents to the Plaintiff as they were approved for release under FOIA. Janosek Decl. ¶ 13.

7. NSA's FOIA Office further informed Plaintiff that if it wanted NSA to conduct a new review of these two previously documents, then it should notify NSA's FOIA Office. NSA's FOIA Office then explained why certain information in these two documents was withheld in the prior FOIA partial releases. Further, NSA's FOIA Office notified Plaintiff as to its right to appeal the withholding of information in these two documents. Janosek Decl. ¶ 13.

8. Finally, the FOIA Office informed Plaintiff that the remaining responsive information had been assigned for review to determine what information could be released and that NSA would finish this review as expeditiously as possible. Janosek Decl. ¶ 13.

9. Plaintiff did not request that NSA re-review the two previously released documents (discussed in ¶¶ 6-7, above), nor did Plaintiff appeal the withholdings in the two documents that NSA released along with its letter of August 14, 2009. Janosek Decl. ¶ 14.

10. By letter dated October 26, 2009, NSA's FOIA Office informed Plaintiff that it had completed its processing of Plaintiff's FOIA request. In this letter, NSA informed Plaintiff that it had conducted a thorough search of its files, but it could not locate any records responsive to item 2 of Plaintiff's request. NSA further informed

Plaintiff that it had located 3 documents consisting of 26 pages that were response to items 1 and 3 of Plaintiff's request. Janosek Decl. ¶ 15.

11. Specifically, regarding item 3 of the FOIA request, NSA informed Plaintiff that there were two responsive documents, but they would be withheld in their entirety based on the fifth exemption of the FOIA because the information contained in these two documents were covered by the deliberative process privilege. Additionally, information in both documents was exempt from release based on the third exemption of the FOIA because the information was protected from release by statute. Further, information in one of these two documents was also exempt based on the first exemption of the FOIA because the information was currently and properly classified in accordance with the governing executive order.

12. These two documents were draft versions of NSA policies, and they were not finalized at the time the Agency conducted its search for records responsive to the Plaintiff's June 25, 2009 FOIA request. In a Supplemental Production dated August 30, 2011, NSA released the finalized versions of these two policies, NSA/CSS Policy 1-58 and IAD Management Directive 20, to the Plaintiff with redactions (pursuant to FOIA Exemptions 1 and 3) of classified information (for NSA/CSS Policy 1-58 only) and information protected from release by statute. Janosek Decl. ¶ 15 & n.2.

13. Finally, the NSA's October 26, 2009 letter informed Plaintiff that there was one document that was responsive to item #1 of its request. NSA informed Plaintiff that it had forwarded this document to the National Security Council for a release determination. Janosek Decl. ¶ 15.

14. The October 26, 2009 letter also notified Plaintiff of its right to appeal NSA's determinations that there were no documents responsive to item #2 of its request, and its determination that the two documents responsive to item #3 were exempt in their entirety. Janosek Decl. ¶ 16

15. By letter November 24, 2009, Plaintiff appealed these two NSA determinations. Janosek Decl. ¶ 17. Plaintiff did not, however, challenge the sufficiency of NSA's search for records responsive to item 3 of Plaintiff's FOIA request. *Id.*

16. NSA placed Plaintiff's appeal in its appeal queue for processing. On February 4, 2010, before NSA had processed Plaintiff's appeal, Plaintiff filed a civil action regarding its FOIA request to NSA. At that time, NSA ceased processing Plaintiff's appeal. Janosek Decl. ¶ 17.

17. On March 25, 2010, Defendants filed a motion to dismiss Counts III and IV of the Complaint, and to dismiss all claims brought against the National Security Council.

18. This Court granted the motion to dismiss on July 7, 2011, dismissing Counts III and IV of the Complaint and dismissing the National Security Council from this action.

DATED: October 11, 2011

Respectfully submitted,

TONY WEST
Assistant Attorney General

RONALD C. MACHEN
United States Attorney

ELIZABETH J. SHAPIRO
Deputy Branch Director

/s/Joshua Wilkenfeld
JOSHUA WILKENFELD
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W.
Washington, D.C. 20530
Tel: (202) 305-7920
Fax: (202) 616-8470
Email: joshua.i.wilkenfeld@usdoj.gov

Counsel for Defendants

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

_____)	
ELECTRONIC PRIVACY)	
INFORMATION CENTER)	
)	
Plaintiff,)	
)	
v.)	No. 1:10-cv-00196-BAH
)	
THE UNITED STATES NATIONAL)	
SECURITY AGENCY)	
)	
Defendant.)	
_____)	

PLAINTIFF’S STATEMENT OF MATERIAL FACTS NOT IN GENUINE DISPUTE

In accordance with Local Civil Rule 7(h) (LCvR7(h)), Plaintiff Electronic Privacy Information Center (“EPIC”) submits this statement of material facts not in genuine dispute in support of its cross motion for summary judgment.

1. In January 2008, National Security Presidential Directive 54 (NSPD 54) was issued by then-President George W. Bush, but not released to the public.
2. The NSA has been involved with the development and execution of cybersecurity policy pursuant to NSPD 54 since its issuance.
3. The NSA is in possession of NSPD 54, the Comprehensive National Cybersecurity Initiative, and related records.
4. On June 25, 2009, EPIC filed a FOIA request with the NSA, seeking (1) the text of the National Security Presidential Directive 54 otherwise referred to as the Homeland Security Presidential Directive 23, (2) the full text, including previously unreported sections, of the Comprehensive National Cybersecurity Initiative, as well as any executing protocols distributed to the agencies in charge of its implementations, and (3)

any privacy policies related to either the Directive, the Initiative, including but not limited to, contracts or other documents describing privacy policies for information shared with private contractors to facilitate the Comprehensive National Cybersecurity Initiative.

5. EPIC's June 25, 2009 FOIA request included a request for expedited processing, news media fee status, and a fee waiver.
6. The NSA acknowledged receipt of EPIC's FOIA request on July 1, 2009 and assigned it case number 58987.
7. The NSA further granted EPIC's request for news media fee status and for a fee waiver, but denied EPIC's request for expedited processing. The NSA did not make a substantive determination as to EPIC's FOIA request.
8. On July 20, 2009 EPIC appealed the NSA's denial of expedited processing and for failing to meet their deadlines for document disclosure as prescribed by the FOIA.
9. On August 12, 2009, the NSA granted EPIC's request for expedited processing.
10. The NSA represented that the search for documents was complete by letter dated August 14, 2009. The NSA included two documents that were responsive to category 3 of EPIC's FOIA request and that had previously been released with redactions pursuant to FOIA Exemption (b)(1) (classified information) and FOIA exemption (b)(3) (information protected from release by statute).
11. The NSA further stated that it was reviewing other responsive documents for release.
12. On October 26, 2009, 73 days after the search for records was completed, the NSA sent a letter to EPIC explaining that no records were found in response to category 2 of EPIC's FOIA request.

13. The NSA's October 26, 2009 letter also stated that three additional documents were found in response to categories 1 and 3 of EPIC's FOIA request. In regard to two of the documents, the NSA asserted (a) both were to be withheld in their entirety under FOIA Exemption (b)(5) (deliberative process privilege), (b) one was to be withheld under FOIA Exemption (b)(1) (classified information), and (c) portions of both documents were to be withheld partially under FOIA Exemption (b)(3) (information protected from release by statute).
14. Finally, the last sentence of the NSA's October 26, 2009 letter stated that the third document found in response to EPIC's FOIA request would be withheld because it did not originate with the NSA, and that the NSA was referring it to the National Security Council "for review and direct response to [EPIC]."
15. The National Security Council is not subject to the FOIA.
16. EPIC transmitted an appeal to the NSA on November 24, 2009, challenging (a) the NSA's assertion that there were no responsive documents to category 2 of EPIC's FOIA request, (b) the NSA's full withholding of the two documents identified in the first part of the NSA's October 26, 2009 letter, and (c) the NSA's full response to the document identified in the last sentence of the NSA's October 26, 2009 letter.
17. The NSA acknowledged receipt of EPIC's FOIA appeal on December 18, 2009.
18. No further communication was received from the NSA regarding EPIC's FOIA request.
19. On February 4, 2010, EPIC filed the immediate action in the United States District Court for the District of Columbia.
20. EPIC's complaint alleged that (a) the NSA failed to comply with the FOIA's statutory deadlines and failed to disclose responsive agency records, (b) the National Security

Council failed to disclose responsive agency records, and (c) that the NSA violated the Administrative Procedure Act by referring part of EPIC's FOIA request to an entity that was not subject to the FOIA.

21. On March 25, 2010, the NSA moved to dismiss EPIC's complaint in relation to the claim against the National Security Council and the Administrative Procedure Act claim.
22. EPIC opposed the NSA's motion to dismiss on April 8, 2010.

The Court granted the NSA's motion on July 7, 2011. The Court further ruled that the NSA's referral of the FOIA request to the National Security Council did not relieve the NSA of its continuing obligation to respond to the request.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY)	
INFORMATION CENTER)	
)	
Plaintiff,)	
)	
v.)	No. 1:10-cv-00196-BAH
)	
THE UNITED STATES NATIONAL)	
SECURITY AGENCY)	
)	
Defendant.)	

**PLAINTIFF’S STATEMENT OF GENUINE ISSUES IN OPPOSITION TO
DEFENDANT’S STATEMENT OF MATERIAL FACTS**

In accordance with LCvR 7(h), Plaintiff the Electronic Privacy Information Center submits this statement of genuine issues in opposition to Defendant’s statement of material facts.

11. Defendant’s alleged fact: “Specifically, regarding item 3 of the FOIA request, NSA informed Plaintiff that there were two responsive documents, but they would be withheld in their entirety based on the fifth exemption of the FOIA because the information contained in these two documents were covered by the deliberative process privilege. Additionally, information in both documents was exempt from release based on the third exemption of the FOIA because the information was protected from released by statute. Further, information in one of these two documents was also exempt based on the first exemption of the FOIA because the information was currently and properly classified in accordance with the governing executive order.”

Genuine Issue: Plaintiff disputes Defendant’s alleged fact insofar as it states legal conclusions.

12. Defendant's alleged fact: "These two documents were draft versions of NSA policies, and they were not finalized at the time the Agency conducted its search for records responsive to the Plaintiff's June 25, 2009 FOIA request..."

Genuine Issue: Plaintiff disputes Defendant's alleged fact insofar as it is a legal conclusion.

13. Defendant's alleged fact: "Finally, the NSA's October 26, 2009 letter informed Plaintiff that there was one document that was responsive to item #1 of its request. NSA informed Plaintiff that it had forwarded this document to the National Security Council for a release determination."

Genuine Issue: Plaintiff disputes the second sentence of Defendant's alleged fact insofar as it is inconsistent with the October 26, 2009 letter, which states that the document "did not originate with the agency," and that "the subject document has been referred to the National Security Council for review and direct response to you."

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

ELECTRONIC PRIVACY)	
INFORMATION CENTER)	
)	
Plaintiff,)	
)	
v.)	Case No. 1:10-cv-00196-BAH
)	
NATIONAL SECURITY AGENCY)	
)	
)	
)	
Defendant.)	

**DEFENDANT’S STATEMENT OF GENUINE ISSUES IN OPPOSITION TO
PLAINTIFF’S STATEMENT OF MATERIAL FACTS**

Pursuant to Local Civil Rule 7(h) of the Rules of the United States District Court for the District of Columbia, defendant National Security Agency hereby submits this statement of genuine issues in opposition to Plaintiff’s statement of material facts.

1. Paragraph 2 of Plaintiff’s statement of material facts asserts that “The NSA has been involved with the development and execution of cybersecurity policy pursuant to NSPD 54 since its issuance.” Contrary to the requirements of the Local Rules, Plaintiff did not “include references to the parts of the record relied on to support th[is] statement.” Local Civil Rule 7(h)(1). Instead, as described in the declaration of Diane M. Janosek (attached to NSA’s Motion for Summary Judgment), “NSA/CSS has a role in the [Comprehensive National Cybersecurity Initiative], but any operational or amplifying details are properly and currently classified in accordance with E.O. 13526 and/or protected from release by statute, specifically, Section 6 of the National Security Agency

Act of 1959 . . . ; and/or Section 102A(i)(1) of the Intelligence Reform and Terrorism Prevention Act of 2004.” Janosek Decl. ¶ 9. In any event, NSA’s precise involvement in the development and execution of cybersecurity policy does not constitute a material fact at issue in this dispute.

DATED: December 8, 2011

Respectfully submitted,

TONY WEST
Assistant Attorney General

RONALD C. MACHEN
United States Attorney

ELIZABETH J. SHAPIRO
Deputy Branch Director

/s/Joshua Wilkenfeld
JOSHUA WILKENFELD
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W.
Washington, D.C. 20530
Tel: (202) 305-7920
Fax: (202) 616-8470
Email: joshua.i.wilkenfeld@usdoj.gov

Counsel for Defendants

**U.S. District Court
 District of Columbia (Washington, DC)
 CIVIL DOCKET FOR CASE #: 1:10-cv-00196-BAH**

ELECTRONIC PRIVACY INFORMATION CENTER v.
 NATIONAL SECURITY AGENCY et al
 Assigned to: Judge Beryl A. Howell
 Case in other court: USCA, 13-05369
 Cause: 05:552 Freedom of Information Act

Date Filed: 02/04/2010
 Date Terminated: 11/19/2013
 Jury Demand: None
 Nature of Suit: 895 Freedom of
 Information Act
 Jurisdiction: U.S. Government Defendant

Date Filed	#	Docket Text
09/09/2013		<p>MINUTE ORDER (paperless) Pending before the Court are the <u>12</u> Defendant's Motion for Summary Judgment and the <u>13</u> Plaintiff's Cross-Motion for Summary Judgment, in which the parties dispute whether the "National Security Presidential Directive 54 ("NSPD 54") and related agency records," are exempt from disclosure under the Freedom of Information Act ("FOIA"). The parties assume in their briefing that the requested documents are "agency records" subject to FOIA disclosure, unless one of nine specific exemptions applies. See 5 U.S.C. § 552(b)(1)-(9); Pl's Mem. in Supp. of Cross-Mot. for Summ. J ("Pl's Mem.") at 2, ECF No. 13-1; Def's Mem. in Supp. of Mot. for Summ. J. ("Def's Mem.") at 3, ECF No. 12-1. In <i>Judicial Watch v. United States Secret Service</i>, Civil No. 11-5282, 2013 U.S. App. LEXIS 18119 (D.C. Cir. August 30, 2013), the United States Court of Appeals for the District of Columbia Circuit determined that certain White House Access Control System ("WHACS") records, which were "arguably created by White House staff... in the course of carrying out the constitutional, statutory, official, and ceremonial duties of the President," <i>id.</i> at 54-55 (internal quotations and citations omitted), were not "agency records" subject to the FOIA. In reaching this conclusion, the D.C. Circuit applied the modified control test set forth in <i>United We Stand America, Inc. v. IRS</i>, 359 F.3d 595 (2004), which had previously been applied only to Congressional records, 2013 U.S. App. LEXIS 18119 at 40-41 n. 21. A critical focus of the modified control test is whether "the non-covered entity here, the White House has manifested a clear intent to control the documents." <i>Id.</i> at 37. If the parties would like the opportunity to address the relevance, if any, of the D.C. Circuit's recent decision in <i>Judicial Watch</i> to the issues raised by the withholding of the requested documents in the instant case, the parties are directed to submit jointly, by September 16, 2013, a schedule for supplemental briefing. Signed by Judge Beryl A. Howell on 09/09/2013. (lcbah2) (Entered: 09/09/2013)</p>
09/09/2013		<p>Set/Reset Deadlines: Joint schedule for supplemental briefing due by 9/16/2013. (tg,) (Entered: 09/09/2013)</p>

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

_____)	
ELECTRONIC PRIVACY)	
INFORMATION CENTER)	
)	
Plaintiff,)	
)	
v.)	No. 1:10-cv-00196-BAH
)	
NATIONAL SECURITY AGENCY)	
)	
Defendant.)	
_____)	

JOINT STATUS REPORT

On September 9, 2013, this Court entered a minute order, which directed: “[I]f the parties would like the opportunity to address the relevance, if any, of the D.C. Circuit’s recent decision in *Judicial Watch* [*v. U.S. Secret Service*, Civil No. 11-5282, 2013 U.S. App. LEXIS 18119 (D.C. Cir. Aug. 30, 2013),] to the issues raised by the withholding of the requested documents in the instant case, the parties are directed to submit jointly, by September 16, 2013, a schedule for supplemental briefing.” The parties have conferred and agree that no supplemental briefing is necessary.

Date: September 13, 2013

Respectfully submitted,

/s/ Marc Rotenberg
MARC ROTENBERG
AMIE STEPANOVICH
Electronic Privacy Information
Center
1718 Connecticut Ave., NW
Suite 200
Washington, D.C. 20009
(202) 483-1140

STUART F. DELERY
Assistant Attorney General

RONALD C. MACHEN, JR.
United States Attorney

ELIZABETH J. SHAPIRO
Deputy Branch Director,
Federal Programs Branch

Counsel for Plaintiff

/s/ Gregory Dworkowitz
GREGORY DWORKOWITZ

(N.Y. Bar Registration No. 4796041)
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W.
Washington, DC 20530
Tel: (202) 305-8576
Fax: (202) 616-8470
E-mail: gregory.p.dworkwitz@usdoj.gov

Counsel for Defendant