

**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

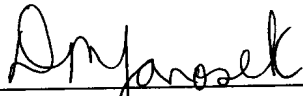
the search because they would be executing aspects of the CNCI. The search for records responsive to item #2 was conducted by the same organizations that searched for records responsive to item #3 of the Plaintiff's FOIA request, but none of them located any such "executing protocols" that were "distributed"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

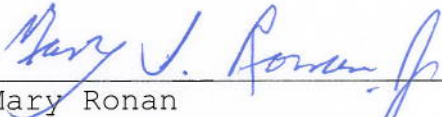
13. While it is possible to segregate parts of NSPD-54 that can be released consistent with FOIA exemption (b)(1) without adversely affecting the national security of the United States, NSPD-54 should be withheld in full under FOIA exemption

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.