IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER, Plaintiff, v. UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Defendant.	)	Civil Action No. 12-0333 (GK)

MEMORANDUM IN SUPPORT OF
DEFENDANT'S MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

INDEX OF EXHIBITS

INTRODUCTION

This case involves a request for records pursuant to the Freedom of Information Act, 5 U.S.C. § 552. The initial request submitted by the Electronic Privacy Information Center ("EPIC") to the United States Department of Homeland Security ("DHS") sought broad categories of information related to a then-ongoing cyber security pilot program, the Defense Industrial Base (DIB) Cyber Pilot. The broadest of these categories included "all analyses, legal memoranda, and related records" regarding the pilot program. After DHS had collected more than 10,000 pages of potentially responsive documents requiring individual review, EPIC narrowed the scope of the FOIA request at issue to exclude all draft documents from the scope of its request. EPIC also narrowed the broadest category, described above, so that it would include "all legal and technical analyses, including legal memoranda, regarding the DIB cyber pilot."

DHS produced non-exempt records to EPIC on April 15, 2013. After the production, DHS conducted a supplemental search based on questions raised by EPIC and supplemented its production of documents to EPIC on August 16, 2013. In total, DHS produced 1386 pages of documents, including some released in full and some released in part, and withheld in full 362 pages of documents.

Based on defendant's accompanying declarations and the Vaughn Index, DHS has satisfied all its statutory obligations under FOIA. After conducting a reasonable search, DHS has released all segregable, non-exempt responsive material in the records it located, and withheld only exempt material pursuant to FOIA Exemptions 1, 3, 4, 5, 6, and 7 see id. §§ 552(b)(1), (b)(3), (b)(4), (b)(5), (b)(6), (b)(7).[1] Accordingly, this Court should grant defendant's motion for summary judgment.

---

[1] EPIC has represented that it does not challenge DHS's Exemption 6 withholdings. As a result, this memorandum will not speak to and the Court need not address Exemption 6.

BACKGROUND

A. The Defense Industrial Base Cyber Pilot

The Defense Industrial Base Cyber Pilot—called the "DIB Cyber Pilot" for short—was a cyber-security pilot program jointly conducted by the Department of Defense and defendant the Department of Homeland Security ("DHS" or "defendant"). The aim of the program was to protect U.S. critical infrastructure. Under the pilot, the Government furnished classified threat and technical information to voluntarily participating Defense Industrial Base (DIB) companies or their Commercial Service Providers (CSPs). This sensitive Government-furnished information enabled the DIB companies, or the CSPs on behalf of their DIB customers, to counter known malicious activity and to protect Department of Defense program information.

B. DHS Processes EPIC Request By Conducting Search for Responsive Records, Coordinating the Processing of Records by Multiple Federal Agencies, and Releasing Hundreds of Pages of Partially-Redacted Records

1. EPIC's July 26, 2011 Request to DHS, and DHS's Initial Response

The DHS Privacy Office ("DHS Privacy") responded to EPIC's FOIA request on August 3, 2011, denying the request in part and indicating that it had referred the remainder of the request to the National Protection & Programs Directorate ("NPPD") FOIA Office for processing and direct response because the documents requested were most likely to be located within NPPD offices.[2] NPPD leads the national effort to protect and enhance the resilence of the nation's physical and cyber infrastructure. NPPD includes several subcomponents, including

[2] As noted in footnote 2, infra, DHS denied category (e) of EPIC's request because after conducting a search DHS had been unable to locate or identify any responsive records. EPIC did not appeal that determination.

the Office of Cybersecurity and Communications (CS&C), which is charged with assuring the security, resiliency, and reliability of the nation's cyber and communications infrastructure.

On January 5, 2012, EPIC sent by facsimile to the NPPD FOIA Office a letter that purported to constitute a FOIA appeal with regard to the remaining four categories of plaintiff's FOIA request. NPPD FOIA had already began searching for responsive documents. After receiving the facsimile, an NPPD FOIA Specialist with NPPD updated an EPIC representative by telephone regarding the status of the FOIA request, and communicated that DHS was processing the request.

Rather than wait for the administrative processing to be completed, EPIC filed this lawsuit on March 1, 2012. DHS filed an answer on May 1, 2012. In the meantime, DHS continued to search for responsive documents. NPPD FOIA officers met with DHS subject matter experts who were familiar with the DIB Cyber Pilot. Together, they identified the DHS offices that were likely to have responsive records, and tasked these offices with conducting electronic and physical record searches for potentially responsive documents. Those offices were: a) the NPPD Office of the Under Secretary, including the Deputy Under Secretary and the Deputy Under Secretary for Cybersecurity; b) the NPPD Office of Privacy (NPPD Privacy); and c) the NPPD Office of Cybersecurity & Communications (CS&C), which as noted above, is responsible for enhancing the security, resiliency, and reliability of the nation's cyber and communications infrastructure.

In addition to tasking the NPPD Office of the Under Secretary, NPPD Privacy, and CS&C with searches, NPPD provided the original FOIA request to the DHS Office of General Counsel and the Office of Selective Acquisitions (OSA) within the DHS Office of the Chief Procurement Officer for review and possible response. The Office of the Chief Procurement Officer is located within the office of the DHS Under Secretary for Management, which is

responsible for the DHS budget, appropriations, expenditure of funds, accounting and finance, and procurement, among other functions. OSA is responsible for overseeing the execution of classified procurements.

In April 2012, working with subject matter experts, NPPD FOIA crafted the following keywords to electronically search for responsive documents, which were provided to NPPD components to use in their initial search: Monitor + Defense contractors; Defense contractors + internet; DIB Pilot; NSA Pilot; MOA + DHS + NSA; PIA + DIB; PIA + NSA; ISPs Monitor; Monitor Internet + NSA. In addition to these keywords, in early May 2012, NPPD FOIA advised NPPD components to use the following additional keywords in their electronic search for responsive documents: NSA Pilot; NSA +[name of DIB company]; NSA +[name of DIB company]; NSA + [name of DIB company]; NSA + defense + pilot; NSA + AT&T; NSA + Century Link; NSA + Monitor + Internet; NSA + DHS + pilot; and DOD + pilot. Recognizing that employees often devise their own methods to store their own documents and records, NPPD FOIA instructed each employee to conduct searches utilizing the employee's knowledge of how and where they stored their own documents and records. Thus, employees who organized their documents topically into folders and subfolders had no need to run keyword searches because they could retrieve any responsive documents by going to the specified folder location.

By the end of July 2012, NPPD had gathered more than 16,000 pages of potentially responsive documents. DHS assigned a team of FOIA specialists and attorneys to review the documents that had been gathered to remove duplicates and cull out documents that had been identified by DHS's electronic keywords search but plainly were not responsive to EPIC's request. Working diligently for several weeks to review the more than 16,000 pages of potentially responsive documents, DHS FOIA specialists and attorneys who had been assigned to the project removed approximately 6,000 documents as either duplicative or not responsive to

the request. In other words, after their review of the 16,000 documents, the team of DHS FOIA specialists and attorneys identified 10,000 documents that were potentially responsive to EPIC's FOIA request.

2. After DHS Locates More Than 10,000 Pages of Potentially Responsive Records, EPIC Narrows the Scope of Its Request; DHS Processes the Records in Response to the Revised Request

After gathering more than 10,000 pages of potentially responsive records, DHS furnished EPIC with detailed information about these documents and the DIB Cyber Pilot in order to allow EPIC to identify with increased particularity the records that it sought. On August 31, 2012, EPIC modified its request in two ways. First, EPIC modified its request by revising the phrasing of the third category of the request, changing the language from "all analyses, legal memoranda, and related records regarding the [DIB Cyber Pilot]" to "all legal and technical analyses, including legal memoranda, regarding the DIB cyber pilot." Second, EPIC excluded draft documents from the record request. Thus, EPIC's revised request sought the following, (excluding draft documents):

> (a) all contracts and communications with Lockheed Martin, CSC, SAIC, Northrop Grumman or other defense contractors regarding the DIB Cyber Pilot;
>
> (b) all contracts and communications with AT&T, Verizon, and CenturyLink or any other Internet Service Providers regarding the DIB Cyber Pilot;
>
> (c) all legal and technical analyses, including legal memoranda, regarding the DIB Cyber Pilot; and
>
> (d) any memoranda of understanding between NSA and DHS or any other government agencies or corporations regarding the DIB Cyber Pilot.

Upon receiving EPIC's revised request, DHS tasked its Privacy Office to assist with completing the processing of revised FOIA request. DHS's Privacy Office conducted a page-by-

page and line-by-line review of the potentially responsive documents to identify those records that were actually responsive to EPIC's revised FOIA request. This entailed segregating exempt portions of the responsive records from the non-exempt portions of them. Given the sensitive and classified nature of the records responsive to EPIC's FOIA request, DHS exercised extraordinary care to process these documents to ensure that the constraints on the disclosure of classified and law enforcement sensitive information were properly observed, and that no inadvertent disclosures of classified materials were made.

As a direct result of its careful and deliberative work, on April 15, 2013, DHS completed its second final response to EPIC's revised FOIA request. That response consisted of 1,276 pages of materials, of which 117 pages of records were released in their entirety and 1,159 pages were partially releasable under FOIA exemptions b(6) and 7(E). On April 15, 2013, DHS, through its counsel at DOJ, transmitted this response directly to EPIC.

Since production of these responsive documents, DHS has made itself available to answer EPIC's questions regarding the production. EPIC sent DHS, through DHS's counsel, a list of 17 documents that EPIC believed were missing from the production. DHS reviewed the list of documents identified by EPIC and determined that 14 of the 17 documents were draft documents that were excluded from the production pursuant to the parties' August 31, 2012 agreement.

On August 14, 2013, DHS issued a supplemental response to EPIC's revised FOIA request, providing EPIC with the remaining three documents it had identified as missing from the production. A total of 84 pages of records were provided to EPIC. Of the 84 pages, 25 pages were re-released documents from the April 15, 2013 production after DHS determined to make certain additional discretionary releases of information. Fifty-nine pages of the supplemental

response had not been previously provided to EPIC, including 26 pages of documents that corresponded with the three documents EPIC had identified as missing.

C. DHS Coordinates the Processing of Records by Multiple Federal Agencies, and Releases All Segregable, Non-Exempt, Responsive Records

Of the partially redacted documents produced by DHS, EPIC has indicated that it challenges all redactions except for the (b)(3) and (b)(6) redactions that were applied to protect employee identification and contact information; the challenged withholdings are described in greater detail in the Vaughn index appended to Mr. Holzer's second declaration. EPIC also challenges the withholding of the documents that DHS has withheld in full, which are also listed and described in the Vaughn index. See id.

LEGAL STANDARD

Under Rule 56 of the Federal Rules of Civil Procedure, summary judgment must be granted when the record evidence demonstrates that "there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a); Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 247 (1986). FOIA cases are typically and appropriately decided on motions for summary judgment. Gold Anti-Trust Action Comm., Inc. v. Bd. of Governors of Fed. Reserve Sys., 762 F. Supp. 2d 123, 130 (D.D.C. 2011); Defenders of Wildlife v. U.S. Border Patrol, 623 F. Supp. 2d 83, 87 (D.D.C. 2009).

An agency that withholds information pursuant to a FOIA exemption bears the burden of justifying its decision, Petroleum Info. Corp. v. Dep't of the Interior, 976 F.2d 1429, 1433 (D.C. Cir. 1992) (citing 5 U.S.C. § 552(a)(4)(B)), and may justify its withholdings by submitting declarations and an index of all materials withheld.[3] Gallant v. NLRB, 26 F.3d 168, 172 (D.C.

[3] What is now commonly known as a "Vaughn index" can take the form of an itemized index, correlating each withheld document or portion of a document with a specific FOIA exemption

Cir. 1994). FOIA "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) (citation omitted). In enacting FOIA, Congress recognized "that legitimate governmental and private interests could be harmed by [the] 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). Thus, although FOIA generally promotes disclosure, it recognizes "that public disclosure is not always in the public interest." Baldrige v. Shapiro, 455 U.S. 345, 352 (1982). As the Supreme Court has stressed, the statutory exemptions must be construed "to have meaningful reach and application." John Doe Agency v. John Doe Corp., 493 U.S. 146, 152 (1989).

In support of their motion for summary judgment, defendant submits several declarations and a Vaughn index. These materials demonstrate that DHS properly segregated and withheld exempt information from release pursuant to FOIA Exemptions 1, 2, 3, 5, 6, and 7. Because these declarations and index describe the withheld material with reasonable specificity, show that this material falls within these exemptions, and are submitted in good faith, the Court should enter summary judgment for DHS.

---

and the agency's nondisclosure justification. Vaughn v. Rosen, 484 F.2d 820, 827 (D.C. Cir. 1973). It is but one of multiple options available to an agency seeking to sustain its evidentiary burden of proving that withheld information falls within a FOIA exemption. See, e.g., Gallant v. NLRB, 26 F.3d 168, 172-73 (D.C. Cir. 1994) (noting that an agency's evidence may take "the form of an in camera review of the actual documents, something labeled a 'Vaughn Index,' a detailed affidavit, or oral testimony"). "Indeed, an agency may . . . submit other measures in combination with or in lieu of the index itself." Judicial Watch, Inc. v. FDA, 449 F.3d 141, 146 (D.C. Cir. 2006).

ARGUMENT

A. The Court Should Enter Judgment for the DHS as to the Adequacy of Its Search for Documents Responsive to EPIC'S FOIA Request Because It Conducted a Reasonable Search and Produced Responsive Documents

1. FOIA Requires Agencies to Conduct Reasonable, Not Exhaustive, Searches

In a FOIA case, a court may award summary judgment to an agency upon a showing that it "conducted a search reasonably calculated to uncover all relevant documents." Weisberg v. U.S. Dep't of Justice, 705 F.2d 1344, 1351 (D.C. Cir. 1983). In other words, FOIA requires the agency to make "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). The adequacy of a search is judged not by its results "but by the appropriateness of the methods used" to execute it. Iturralde v. Comptroller of the Currency, 315 F.3d 311, 315 (D.C. Cir. 2003). Thus, "in assessing the reasonableness of a search, a court is not guided by whether the search actually uncovered every document" or even "whether the search was exhaustive." Brannum v. Dominguez, 377 F. Supp. 2d 75, 79 (D.D.C. 2005) (internal quotation marks and citation omitted); see also Meeropol v. Meese, 790 F.2d 942, 952-53 (D.C. Cir. 1986) (explaining that "a search is not unreasonable simply because it fails to produce all relevant material"). Rather, the question is whether the search itself was adequate notwithstanding the fact that other responsive documents may exist. Steinberg v. U.S. Dep't of Justice, 23 F.3d 548, 551 (D.C. Cir. 1994). An agency need not search every record system, although it "cannot limit its search to only one . . . if there are others that are likely to turn up the information requested." Oglesby, 920 F.2d at 68. In short, the agency's search is measured against a standard of reasonableness as applied to the specific FOIA request at issue. See Campbell v. U.S. Dep't of Justice, 164 F.3d 20, 27 (D.C. Cir. 1998); Lazaridis v. U.S. Dep't of

Justice, 766 F. Supp. 2d 134, 140-41 (D.D.C. 2011) ("[W]hen an agency's search is questioned, the Court must determine the adequacy of the agency's search, guided by principles of reasonableness.").

An agency may satisfy its summary judgment burden in a FOIA action by submitting affidavits or declarations that "explain in reasonable detail and in a non-conclusory fashion the scope and method of the agency's search." Swope v. U.S. Dep't of Justice, 439 F. Supp. 2d 1, 5 (D.D.C. 2006); see also Perry v. Block, 684 F.2d 121, 127 (D.C. Cir. 1982) (explaining that the affidavits need not "set forth with meticulous documentation the details of an epic search for the requested records"). The process of conducting a reasonable search requires "both systemic and case-specific exercises of discretion and administrative judgment and expertise" and "is hardly an area in which the courts should attempt to micro manage the executive branch." Schrecker v. U.S. Dept't of Justice, 349 F.3d 657, 662 (D.C. Cir. 2003) (internal quotation marks and citation omitted). Therefore, in evaluating the adequacy of a search, courts 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) (internal quotation marks and citation omitted).

2. DHS's Search Was Reasonably Calculated to Locate Responsive Records

As described in the declaration submitted by James Holzer, Second Declaration of James V.M.L. Holzer ("Tab A"), DHS conducted a search reasonably calculated to locate the records responsive to plaintiff's FOIA Request. See Tab A, at ¶¶ 9, 13-43.

DHS's Privacy office tasked the FOIA Office of DHS's National Protection & Programs Directorate ("NPPD") with identifying the offices likely to have documents responsive to EPIC's FOIA request. See id. at ¶10. NPPD leads the national effort to protect and enhance the resilence of the nation's physical and cyber infrastructure. Id. at ¶14. Because of the nature of

the work conducted by NPPD, DHS Privacy tasked NPPD's FOIA office with this project, reasoning that the documents related to the DIB Cyber Pilot were most likely to be located within NPPD offices. Id. at ¶11.

NPPD FOIA officials met with both subject matter experts who had been involved in the DIB Cyber Pilot and attorneys within the DHS Office of General Counsel ("OGC"), who together identified the following NPPD subcomponents most likely to have responsive records: (1) the NPPD Office of the Under Secretary, including the Deputy Under Secretary and the Deputy Under Secretary for Cybersecurity, (2) the NPPD Office of Privacy ("NPPD Privacy"), (3) and the NPPD Office of Cybersecurity and Communications ("CS&C"). Id. at ¶15. NPPD FOIA officials also provided EPIC's FOIA request to the DHS OGC for review and possible response because OGC attorneys provided legal support to the DIB Cyber Pilot staff. Id. at ¶16. NPPD FOIA officials also provided the FOIA request to the Office of Selective Acquisitions ("OSA") within the DHS Office of the Chief Procurement Officer for review and possible response because that OSA, which is located within the office of the DHS Under Secretary for Management and responsible for, among other tasks, DHS budget, appropriations, expenditure of funds, accounting and finance, and procurement, oversees the execution of classified procurements. Id.

After identifying the offices likely to have documents responsive to EPIC's FOIA request, NPPD FOIA officials next worked with DIB Cyber Pilot subject matter experts to identify keyword search terms to be used in electronic document searches by the offices tasked with searching for responsive documents. Id. at ¶17. These individuals crafted 15 search terms that they concluded would be reasonably likely to locate documents potentially responsive to EPIC's FOIA request and provided those keyword terms to all of the offices tasked with conducting a search for responsive documents. See id. In addition to providing the offices and

individuals likely to have responsive documents with keywords to aid in their electronic document, each individual office and employee within the specified office also was instructed to conduct searches of his or her documents utilizing their knowledge of how and where they stored their own documents and records. See id. at ¶18. NPPD FOIA officials provided this instruction to ensure that employees who organized their documents topically into folders or subfolders and had no need to run keyword searches would nonetheless retrieve any responsive documents by going to the specified folder location. Id.

As detailed in the Second Declaration of James Holzer, Tab A, each office tasked with searching for documents responsive to EPIC's FOIA request conducted searches, either electronic, manually or both, to locate documents responsive to the request. See id. at ¶¶20-43. For example, the OUS Executive Secretariat ("OUS ExecSec"), which is responsible for coordinating appropriate and expeditious action on tasks addressed to the Directorate, coordinated the search for responsive documents within OUS. Id. at ¶21. OUS ExecSec program officials and NPPD FOIA officials worked together to identify key OUS staff and officials who were likely to have potentially responsive documents, including any incidental communications with other NPPD staff and officials. Id. at ¶23. Once these individuals were identified, NPPD FOIA officials sent the identified OUS staff a tasking, requesting that each employee conduct a search for documents potentially responsive to EPIC's FOIA request. Id. These OUS employees were provided with the list of 15 keyword search terms crafted by NPPD FOIA officials and DIB Cyber Pilot subject matter experts, which they used to locate potentially responsive documents. Id.

In addition to conducting a search of OUS employees' files, OUS ExecSec staff conducted an electronic search of a Microsoft Access database

B. Because DHS Properly Withheld Exempt Information Pursuant to FOIA's Exemptions, The Court Should Enter Summary Judgment for DHS[4]

FOIA requires agencies to release "any reasonably segregable portion of a record . . . after deletion of the portions which are exempt under this subsection." 5 U.S.C. § 552(b). Consistent with this obligation, the DHS has provided plaintiff with as much non-exempt information as possible without compromising the interests in nondisclosure protected by FOIA. [Declaration.] DHS conducted a line-by-line review of ___ documents, individually and as a whole, to identify and release all reasonably segregable, non-exempt portions of the documents. Id. Based on that review, the DHS released all the information that could be reasonably segregated from the information withheld. Id. The remaining exempt material is described in this section.

1. DHS Properly Withheld Classified Information Under Exemption 1.

As detailed below and in the Holzer declaration and accompanying Vaughn index, DHS determined—after reviewing the DIB Cyber Pilot records and consulting with other federal agencies, particularly with the National Security Agency ("NSA")—that certain portions of the records were exempt under 5 U.S.C. § 552(b)(1) and must be withheld. Tab A ¶52. Exemption 1 protects from disclosure 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). In this case, much of the information withheld pursuant to Exemption 1 consists of NSA

[4] For ease of reading, each of the applicable FOIA exemptions invoked by defendants are addressed herein in the order in which they appear in the FOIA statute. Certain information withheld by DHS is exempt from disclosure under more than one Exemption, as DHS's Vaughn index amply demonstrates. See Holzer Decl. Appx. With respect to any record subject to such overlapping claims of exemptions, this Court need only find any one exemption applicable in order to grant summary judgment to the defendant DHS. See Fund for Constitutional Gov't v. Nat'l Archives & Records Serv., 656 F.2d 856, 864 n.19 (D.C. Cir. 1981).

information that was primarily withheld because it would reveal information about that agency's organization, functions, and activities, which is protected from release by FOIA Exemption 3 in conjunction with Section 6 of the NSA Act of 1959, and 18 U.S.C. § 798. Exemption 1 provides a secondary basis for the withholding of this information, with Exemption 3 providing the primary basis for its withholding. The information that was withheld as classified under Exemption 1 is information that, if disclosed, would reveal classified details of NSA activities or would otherwise reveal classified information as specified in the Vaughn index. Tab A ¶54.

Agency decisions to withhold classified information under FOIA are reviewed de novo by the district court, and the agency bears the burden of proving its claim for exemption. See 5 U.S.C. § 552(a)(4)(B); Miller v. Casey, 730 F.2d 773, 776 (D.C. Cir. 1984). Nevertheless, because federal agencies have "unique insights" into the adverse effects that might result from public disclosure of classified information, the courts must accord "substantial weight" to an agency's affidavits justifying classification. Military Audit Project v. Casey, 656 F.2d 724, 738 (D.C. Cir. 1981); cf. Miller, 730 F.2d at 776 (court must "accord *substantial weight* to an agency's affidavit concerning the details of the classified status of the disputed record") (emphasis in original). "'Executive departments responsible for national defense and foreign policy matters have unique insights into what adverse [effects] might occur as a result of public disclosure of a particular classified record.'" Salisbury v. United States, 690 F.2d 966, 970 (D.C. Cir. 1982) (quoting S. Rep. No. 93-1200, at 12 (1974)). Thus, a court "must take seriously the government's predictions about the security implications of releasing particular information to the public." ACLU v. U.S. Dep't of Justice, 265 F. Supp. 2d 20, 28 (D.D.C. 2003).

Indeed, "the court is not to conduct a detailed inquiry to decide whether it agrees with the agency's opinions." Halperin v. CIA, 629 F.2d 144, 148 (D.C. Cir. 1980); see Weissman v. CIA, 565 F.2d 692, 697 (D.C. Cir. 1997) ("Few judges have the skill or experience to weigh the

repercussions of disclosure of intelligence information."). The issue for the Court is whether "on the whole record the Agency's judgment objectively survives the test of reasonableness, good faith, specificity, and plausibility in this field of foreign intelligence in which [the agency] is expert and given by Congress a special role." Gardels v. CIA, 689 F.2d 1100, 1105 (D.C. Cir. 1982).

An agency establishes that it has properly withheld information under Exemption 1 for a particular record if it shows that it has met the classification requirements of the Executive Order in effect when the final classification action on the record was taken. Campbell v. U.S. Dep't of Justice, 164 F.3d 20, 29 (D.C. Cir. 1998). To carry this burden, an agency must simply demonstrate a "logical connection between the information and the claimed exemption …." ACLU, 265 F. Supp. 2d at 29-30.

In this case, records related to the DIB Cyber Pilot were created—and where necessary, classified—between 2009 and 2012. The applicable Executive Orders during this time period were: first, E.O. 13,292, which was in effect from March 2003 until June 2010; and second, E.O. 13,526, which went into partial effect on December 29, 2009 and into full effect on June 25, 2010.[5] Each of these two Executive Orders contains nearly identical requirements for originally classifying information under the terms of their orders, and substantially similar categories of information eligible for classification consideration. Compare E.O. 13,292 §§ 1.1(a) and 1.4 with E.O. 13,526 §§ 1.1(a) and 1.4. The differences between the Executive Orders do not impact the Exemption 1 analysis in this case. This brief principally discusses the most recent Executive Order, E.O. 13,526, because that Executive Order remains in effect and because it was

[5] President Obama signed Executive Order 13,526 on December 29, 2009. Sections 1.7, 3.3, and 3.7 of the order were effective immediately, with the remainder of provisions effective beginning June 25, 2010.

the governing Executive Order during the time in which DHS and other federal agencies reviewed the records in response to plaintiff's requests and determined whether any portions of the records could be released.[6]

Section 1.1 of E.O. 13,526 sets forth four requirements for the original classification of national security information: (1) an original classification authority classifies the information; (2) the U.S. Government owns, produces, or controls the information; (3) the information is within one of eight protected categories listed in section 1.4 of the Order; and (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in a specified level of damage to the national security, and the original classification authority is able to identify or describe the damages. E.O. 13,526 § 1.1(a). In addition information can be classified pursuant to an agency's derivative classification authority where one agency is "reproduc[ing], extract[ing], or summariz[ing] classified information, or . . . apply[ing] classification markings derived from source material" that originated at another agency. E.O. 13,526 § 2.1. In this case, classified information was withheld based on NSA's original classification authority. Certain information that was reproduced, extracted, or summarized by DHS from materials classified by NSA or another federal agency was withheld based on DHS's derivative classification authority. Tab A

According to the Executive Order, information may be considered for classification if "its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security" and if it pertains to one or more of eight specified categories of

---

[6] DHS determined, in consultation with other federal agencies including the Department of Defense and the National Security Agency, that certain information within the classified records no longer required classified treatment pursuant to EO 13,526 and could be declassified. See generally Holzer Decl. ¶¶ 52-58 & Appx. DHS segregated and produced to plaintiff all unclassified and declassified information that was not otherwise exempt under FOIA from within the classified records. Id.

information. Id. § 1.4. Of particular relevance here, the Executive Order provides that information may be classified if it concerns:

> (e) scientific, technological, or economic matters relating to the national security; [or]
>
> (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security.

Id.

The Exemption 1 claims made by DHS here are supported by the Declaration of James Holzer, who explains that the classified records at issue were either classified by NSA, or were withheld as classified by DHS based on its derivative classification authority. Tab A ¶54. As Mr. Holzer explains, DHS worked with other federal agencies, including DOD and NSA, to review records, to segregate information that could be released as unclassified, and to withhold information that remains properly classified. Id. ¶ 55. David J. Sherman, Associate Director for Policy and Records at the National Security Agency, who serves as a TOP SECRET classification authority reviewed the NSA-related records in this case. Id. Mr. Sherman determined that certain information within them meets the criteria for classification and is in fact currently and properly classified at the SECRET level in accordance with E.O. 13526. See id. Working with NSA, DHS officials segregated the unclassified or declassified information and released it, while withholding that information that is currently and properly classified. Id.

Specifically, NSA and DHS determined that certain information within the records is classified under one or both of two sub-sections of E.O. 13526, sub-sections 1.4(e) and 1.4(g). The information in question reveals capabilities and/or vulnerabilities of systems relating to the

national security, specifically electronic networks used by the defense industrial base sector.[7] Some of the information in question is also classified as pertaining to technological matters relating to the national security, namely cybersecurity operations of the federal government and defense contractors. The unauthorized disclosure of the withheld classified information reasonably could be expected to cause identifiable and describable damage to the national security, as discussed in Mr. Holzer's declaration, the Vaughn index, and below.

The purpose of the DIB Cyber Pilot was to evaluate the potential to enhance the cybersecurity of participating DIB critical infrastructure entities and to protect sensitive information and DIB intellectual property that directly supports national defense missions from unauthorized access and exploitation. Tab A ¶6. The DIB Cyber Pilot operated at the classified level; some of the related records are classified at the TOP SECRET level and some are classified at the SECRET level. See id. ¶57. During the DIB Cyber Pilot, DHS and the Department of Defense shared classified threat and technical information with participating DIB companies and internet service providers, in order to enhance the ability of DIB companies'

[7] The defense industrial base sector ("DIB sector") is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements. Tab A ¶4. The DIB sector includes Department of Defense components and defense-industry companies who perform under contract to the Department of Defense. Id.

The DIB sector is a critical component of our national infrastructure. Id. ¶5. The DIB sector provides products and services that are essential to mobilize, deploy, and sustain U.S. military operations. Id. In recent years, as the United States' reliance on information technology has grown, Department of Defense and DHS leaders have recognized that the DIB Sector—like other important national infrastructure sectors—faces a dangerous, growing threat of cyber intrusion, exploitation, and attack. Id. For example, a foreign intelligence agency in 2008 used a thumb drive to penetrate United States classified computer systems. Id. Current cyber security threats include the threat of theft of data from both government and commercial networks, the threat of disruption of communications networks that deny or degrade the use of important government or commercial network, and the threat of destruction, where cyber tools may be used to cause physical damage. Id.

capabilities to safeguard Department of Defense information that resides on, or transits, computer systems operated by DIB companies. Id. ¶6. Release of the classified information would indicate to our adversaries the strengths and/or weaknesses of our systems. Id. ¶58. Our adversaries could then either seek to exploit any identified weaknesses, or engage in countermeasures in order to reduce the effectiveness of said systems. Id. DHS also withheld certain information that would reveal how NSA conducts its mission; the disclosure of this operational information could reasonably be expected to cause serious damage to the national security by potentially jeopardizing certain activities that NSA undertakes in furtherance of its mission. Id.

In sum, Mr. Holzer's declaration and the appended Vaughn index together demonstrate that the information withheld by DHS pursuant to Exemption 1 is specifically authorized under criteria established by an executive order to be kept secret in the interest of national defense or foreign policy, and is in fact properly classified pursuant to such executive order. Cf. 5 U.S.C. § 552(b)(1). Because DHS's description of the harms that would result from the compelled disclosure of this information is more than sufficient to establish its proper classification under Executive Order 13,526, DHS's Exemption 1 claims must be upheld.

2. DHS Properly Asserted Exemption 3 to Protect Materials For Which the National Security Agency Act and 18 U.S.C. § 798 Require Nondisclosure

FOIA Exemption 3 incorporates nondisclosure provisions contained in other federal statutes. 5 U.S.C. § 552(b)(3); Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 755 (1989). Exemption 3 applies to matters "specifically exempted from disclosure by statute . . . [provided that such statute] (i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue; or (ii) establishes particular criteria for withholding or refers to particular types of matters to be withheld." 5 U.S.C. § 552(b)(3). As the

Court of Appeals has explained, "Exemption 3 differs from other FOIA exemptions in that its applicability depends less on the detailed factual contents of specific documents; the sole issue for decision is the existence of a relevant statute and the inclusion of withheld material within that statute's coverage." Goland v. CIA, 607 F.2d 339, 350-51 (D.C. Cir. 1978). Consequently, under Exemption 3, judicial review is limited to whether (1) the withholding statute qualifies as an Exemption 3 statute, and (2) the withheld material satisfies the criteria of the exemption statute. See CIA v. Sims, 471 U.S. 159, 167 (1985); Fitzgibbon v. CIA, 911 F.2d 755, 761 (D.C. Cir. 1990).[8]

NSA invoked Section 6 of the National Security Agency Act of 1959, Pub. L. No. 86-36, 73 Stat. 63 (codified at 50 U.S.C. § 402 note), as one of two relevant statutes within the meaning of Exemption 3. Section 6 provides, in pertinent part, that "nothing in this Act or any other law … shall be construed to require the disclosure of the organization or any function of the National Security Agency, [or] of any information with respect to the activities thereof." *Id.* Section 6 qualifies as a exempting statute under Exemption 3. Founding Church of Scientology of Washington, D.C. v. NSA, 610 F.2d 824, 828 (D.C. Cir. 1979); see Wilner v. NSA, 592 F.3d 60, 72 (2d Cir. 2009). Further, Section 6's protection is "absolute"; the court is not to consider a requesting party's need for the information. Linder v.NSA, 94 F.3d 693, 698 (D.C. Cir. 1996). Section 6 is intentionally broad: The D.C. Circuit has recognized that "[i]n light of the peculiar NSA security needs . . . Congress certainly had rational grounds to enact for the NSA a

[8] "A specific showing of potential harm to national security . . . is irrelevant to the language of [an Exemption Three statute because] Congress has already, in enacting the statute, decided that disclosure of [the specified information] is potentially harmful." Hayden v. Nat'l Sec. Agency, 608 F.2d 1381, 1390 (D.C. Cir. 1979). Nevertheless, even though such a showing is not required, DHS has provided such a showing of potential harm to national security with respect to releasing much if not all of the information protected by Exemption 3 here, as it is also protected by Exemption 1 and a showing of harm has been met. See Tab A ¶¶52-58.

protective statute broader than the CIA's." See Hayden v. NSA/CSS, 608 F.2d 1381, 1390 (D.C. Cir. 1979). Importantly, therefore, a "specific showing of potential harm to national security . . . is irrelevant to the language of [Section 6]. Congress has already, in enacting the statute, decided that disclosure of NSA activities is potentially harmful." Id. To invoke this privilege, NSA must demonstrate only that the information it seeks to protect falls within the scope of section 6 of the NSA Act. NSA's functions and activities are therefore protected from disclosure regardless of whether or not the information is classified.

On behalf of NSA, DHS also made statutory redactions pursuant to 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. Congress enacted this statute to protect the fragile nature of NSA's SIGINT efforts, to include, but not limited to, the existence and depth of signals intelligence-related successes, weaknesses, and exploitation techniques. This statute recognizes the vulnerability of signals intelligence to countermeasures and the significance of the loss of valuable intelligence information to national policymakers and the Intelligence Community.

The redactions of information made by DHS on behalf of NSA consist primarily of employee names, personally identifiable information, and telephone numbers, as well as information relating to the Agency's internal processes, and activities, such as handling

instructions for classified information, activities, relationships, and our foreign partners.[9] That information falls squarely within the scope of 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), "[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, or of the names, titles, salaries, or number of persons employed by [NSA]."

Here, as the Vaughn index makes clear, information redacted by DHS on behalf of NSA undeniably concerns the organizations, function and activities of the NSA. The redacted information relates directly to NSA activities in relation to its Information Assurance mission, and would reveal classified Agency activities in support of its mission. Tab A ¶60. This information is squarely covered by the terms of section 6 of the NSA Act and its disclosure is prohibited. Moreover, given that Congress specifically prohibited the disclosure of classified information related to its communications intelligence activities, NSA determined that its SIGINT activities and functions, and its intelligence sources and methods would be revealed if certain of the withheld information was disclosed.[10]

---

[9] EPIC does not challenge the withholding of employee names, personally identifiable information, and telephone numbers, as that information is also protected by Exemption 6. EPIC does challenge the withholding of NSA's internal processes, and activities, such as handling instructions for classified information, activities, relationships, and our foreign partners.

[10] One of NSA's cryptologic duties is to disseminate Signals Intelligence ("SIGINT") information for national foreign intelligence and counterintelligence purposes. In performing its SIGINT mission, NSA exploits foreign electromagnetic signals to obtain intelligence information necessary to the national defense, national security, or conduct of foreign affairs. NSA has developed a sophisticated worldwide SIGINT collection network that acquires, among other things, foreign and international electronic communications.

3. DHS Properly Withheld Information Under Exemption 4

DHS also withheld certain confidential commercial information pursuant to FOIA Exemption 4. Exemption 4 protects records from disclosure that contain "commercial or financial information obtained from a person and privileged or confidential." 5 U.S.C. § 552(b)(4). To fall within the exemption, records must contain information that is (1) commercial or financial in character, (2) obtained from a person, and (3) privileged or confidential.

Courts have recognized that the terms "commercial" and "financial" should be given their "ordinary meanings" and merely require that the submitter has a "commercial interest" in the records. See Pub. Citizen Health Research Group v. FDA, 704 F.2d 1280, 1290 (D.C. Cir. 1983) and Bd. of Trade v. Commodity Futures Trading Comm'n, 627 F.2d 392, 403 (D.C. Cir.1980)). Under National Parks and Conservation Ass'n v. Morton, 498 F.2d 765 (D.C. Cir. 1974), private commercial information that has been submitted to the government under compulsion is "confidential" for purposes of Exemption 4 if disclosure is likely either "(1) to impair the Government's ability to obtain necessary information in the future; or (2) to cause substantial harm to the competitive position of the person from whom the information was obtained." Id. at 770 (footnote omitted). A slightly different standard applies to private commercial information that is provided to the government voluntarily. Such information is confidential for purposes of Exemption 4 "if it is of a kind that would customarily not be released to the public by the person from whom it was obtained." Critical Mass Energy Project v. Nuclear Regulatory Comm'n, 975 F.2d 871, 879 (D.C. Cir. 1992). These two tests recognize that Exemption 4 is designed to protect the government's interest in the availability and reliability of commercial and financial information obtained from third parties and also to protect the interests of persons who provide such information to the government. See id. at 877–79.

In this case, DHS on behalf of DOD withheld certain information to protect commercial information provided by DIB companies who voluntarily participated in the DIB Cyber Pilot. DHS also withheld proprietary information of the Commercial Service Providers (CSPs) who participated in the pilot. Participation by DIB companies and CSPs in the DIC Cyber Pilot was voluntary, and the information provided by these companies to the government was also done on a voluntary basis, id.

The withheld information meets the element of being "commercial" information because the DIB companies and CSPs have commercial interests in the information. Pub. Citizen Health Research Group, 704 F.2d at 1290. The companies participated in the DIB Cyber Pilot for commercial reasons. According to 2012 study by the Ponemon Institute, the average annualized cost of cybercrime for defense industry companies in 2012 was $21.7 million. See Tab C. Thus, both the DIB companies and the CSPs that serve them have financial stakes in improving their cybersecurity. At the same time, if a company's participation in the DIB Cyber Pilot were publicly known, that company could face increased cyber targeting, exposing the company to greater business or financial loss. Participation in the DIB Cyber Pilot could be viewed as an admission of cyber vulnerability; a company could face competitive disadvantages or market loss if its participation were revealed. Id. To encourage private sector companies to participate in information sharing programs, such as the DIB Cyber Pilot, and also to respect the companies' practice of not publicly disclosing their participation in programs that would acknowledge cyber vulnerabilities, the government must allow the companies to participate confidentially, and thus redact the names or other information that would reveal their confidential participation pursuant to Exemption 4.

With regard to the DIB companies, DOD expressly promised that their participation would be confidential. The confidentiality policy was communicated to the participating pilot

companies both verbally and in written documentation. Tab C. For example, the agreement signed by the pilot companies and the DoD Chief Information Officer states, "[t]he Government acknowledges that information shared by the Company under this program may include extremely sensitive proprietary, commercial, or operational information that is not customarily shared outside of the company, and that the unauthorized use or disclosure of such information could cause substantial competitive harm to the Company that reported that information," and that the government "shall take reasonable steps to protect against the unauthorized use or release of such information (e.g., attribution information and other non-public information)."[11] Id. The publicly available Privacy Impact Assessment also informs the public that DoD will restrict "attribution data" only to those authorized personnel that have a need-to-know such information for duties in support of the DIB CS/IA Program (or other authorized DoD cybersecurity, LE/CI, or other lawful purposes), and that are subject to appropriate nondisclosure obligations.[12] Id. Moreover, as the Herrington declaration explains, details regarding the cyber-security programs of these companies, including their participation in programs such as the DIB Cyber Pilot that might indicate information regarding their cyber vulnerabilities, is information that is not customarily released by the companies. Id.

As the Holzer declaration and Vaughn index explain, the CSPs also customarily treat the withheld information as confidential. For example, in one email partially redacted by DHS, the email author states that "this material and what I am going to tell you is proprietary and

---

[11] The Herrington declaration provides additional details about the confidentiality provisions in the agreement signed by the DIB companies and DoD.

[12] Attribution information is defined in the agreement as: "information that identifies the Company or its programs, whether directly or indirectly, by the grouping of information that can be traced back to the Company (e.g., program description, facility locations, number of personnel, etc.)." Id. (emphasis added).

sensitive." Tab B at doc. 348. The email discusses proprietary information about the CSP's technical capabilities, customers, and views regarding other members of the CSP industry. Id.

4. DHS Properly Protected Material Under Exemption 5, Pursuant to the Deliberative Process Privilege, the Attorney-Client Privilege and the Attorney Work Product Doctrine

Exemption 5 allows an agency to withhold "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than agency in litigation with the agency." 5 U.S.C. § 552(b)(5). Exemption 5 ensures that members of the public cannot "obtain through FOIA what they could not ordinarily obtain through discovery undertaken in a lawsuit against the agency." Schiller v. Nat'l Labor Relations Bd., 964 F.2d 1205, 1208 (D.C. Cir. 1992) (citation omitted), abrogated on other grounds, Milner v. Dep't of Navy, 131 S. Ct. 1259 (2011). As a result, Exemption 5 "exempt[s] those documents . . . normally privileged in the civil discovery context." Id. (citations omitted)). Of the ordinary litigation privileges available to DHS, the deliberative process privilege, the attorney-client privilege, and the attorney-work product doctrine are applicable here.

a. The Deliberative Process Privilege

Documents covered by the deliberative process privilege include those "reflecting advisory opinions, recommendations and deliberations comprising part of a process by which governmental decisions and policies are formulated." NLRB v. Sears, Roebuck & Co., 421 U.S. 132, 150 (1975) (citation omitted). As the Supreme Court has explained:

The deliberative process privilege rests on the obvious realization that officials will not communicate candidly among themselves if each remark is a potential item of discovery and front page news, and its object is to enhance the quality of agency decisions by protecting open and frank discussion among those who make them within the Government. Dept. of Interior v. Klamath Water Users Protective Ass'n, 532 U.S. 1, 8-9 (2001) (internal quotation marks and

citations omitted). FOIA's inclusion of the deliberative process privilege among its exemptions "reflect[s] the legislative judgment that the quality of administrative decision-making would be seriously undermined if agencies were forced to 'operate in a fishbowl' because the full and frank exchange of ideas on legal or policy matters would be impossible." Tax Analysts v. IRS, 117 F.3d 607, 617 (D.C. Cir. 1997).

In order to qualify for the deliberative process privilege, an agency record must satisfy three conditions. It must be "inter-agency or intra-agency," 5 U.S.C. § 552(b)(5), that is, "its source must be a Government agency," Klamath, 532 U.S. at 8; and it must be both "predecisional" and "deliberative." In re Sealed Case, 121 F.3d 729, 737 (D.C. Cir. 1997) (citations omitted). "To establish that a document is predecisional, the agency need not point to an agency final decision, but merely establish what deliberative process is involved, and the role that the documents at issue played in that process." Judicial Watch v. Export-Import Bank, 108 F. Supp. 2d 19, 35 (D.D.C. 2000) (citation omitted). A record is "deliberative" when "it reflects the give-and-take of the consultative process." Wolfe v. Dep't of Health & Human Servs., 839 F.2d 768, 774 (D.C. Cir. 1988) (citation and internal quotation marks omitted) (en banc). "There should be considerable deference to the [agency's] judgment as to what constitutes . . . 'part of the agency give-and-take – of the deliberative process – by which the decision itself is made.'" Chem. Mfrs. Ass'n v. Consumer Prod. Safety Comm'n, 600 F. Supp. 114, 118 (D.D.C. 1984) (quoting Vaughn v. Rosen, 523 F.2d 1136, 1144 (D.C. Cir. 1975)). The agency is best situated "to know what confidentiality is needed 'to prevent injury to the quality of agency decisions . . . .'" Id. at 118 (quoting Sears, 421 U.S. at 151).

Here, DHS properly withheld the contents of inter and intra-agency email communications that reveal "the give-and-take" of the consultative process necessary to develop, implement, and operate a project the magnitude and complexity of the DIB Cyber Pilot. See Tab

A, ¶ 57. For example, email communications among DHS personnel discussing recommendations regarding the development of the DIB Cyber Pilot and an agency employee's opinion regarding the need for potential modifications to the project, see Tab B at doc. 115, are properly withheld under Exemption 5 because they are pre-decisional and deliberative. See also id. at doc. 269 (email communication from DHS program official to other DHS employees, including DHS counsel, outlining the official's recommendations regarding the agency's operational targets through the DIB transition period); id. at doc. 40 (email chain among DHS personnel that contains a DHS employee's opinion regarding, among other issues, the need to consider certain material in developing the DIB Cyber Pilot programs privacy policies and procedures).

The same applies to inter-agency email communications that reveal the consultative process related to the development and operation of the DIB Cyber Pilot program, including policy concerns raised by agency stakeholders. Id. at doc. 431 (email chain among DHS and DOD employees that reveals their opinions and recommendations regarding intra- and inter-agency proposed processes for implementing the DIB Cyber Pilot, including a discussion of policy questions related to potentially modifying the same); id. at doc. 328 (email communications between DHS and DOD personnel regarding the development of the JOIN Cybersecurity Services Pilot PIA, including proposed changes to DHS's application of Paperwork Reduction Act requirements). Plainly, these are the sorts of "advisory opinions, recommendations and deliberations comprising part of a process by which governmental decisions and policies are formulated" and are thus properly protected by the deliberative process privilege. Sears, 421 U.S. at 150.

Similarly, talking points, plans, proposals and briefing papers generally constitute privileged deliberative material. Such papers are typically prepared to assist decisionmakers in

making decisions or in communicating those decisions to the public and the press. See, e.g., Tab A at __; Tab B at docs. ___. Disclosure of "work plans, status reports, briefings, opinion papers, and proposals" would "stifle the candor necessary in an agency's policy making process." Hornbostel v. U.S. Dept. of the Interior, 305 F. Supp. 2d 21, 31 (D.D.C. 2003); see also Thompson v. Dept. of the Navy, 1995 WL 527344, at *4 (D.D.C. 1997); see also Access Reports v. Dept. of Justice, 926 F.2d 1192, 1196-97 (D.C. Cir. 1991) (memorandum regarding "study of how to shepherd the FOIA bill through Congress" protected, as are "communications . . . contributing to deliberations about whether to introduce legislation"); Hunt v. U.S. Marine Corps, 935 F. Supp. 46, 52 (D.D.C. 1996) ("point papers" prepared in the "midst of [agency's] deliberative process to assist officers in their formulation of a final decision" exempt from disclosure); Klunzinger v. IRS, 27 F. Supp. 2d 1015, 1026-27 (W.D. Mich. 1998) (briefing paper for Commissioner exempt).

In this case, DHS properly withheld email communications containing proposed language for responding to a newspaper article on the DIB Cyber Pilot program, see Tab B, at doc. 259 (email communication among DHS program officials and senior leadership discussing a proposed statement by DOD for release to the Washington Post regarding the Cyber Pilot program, including a discussion of specific language to clarify the agency's position regarding the monitoring of certain types of internet traffic); id. at doc. 91 (email communication containing draft language to respond to media inquiry). The agency also properly withheld talking points, proposed agendas, and other briefing papers that were drafted to facilitate both intra and inter-agency discussions of issues related to the development and implementation of the DIB Cyber Pilot. See id. at doc. 284 (email chain among DHS program officials discussing what information to include in talking points on Cyber Storm III, NCIRP, and background information on the DIB Cyber Pilot); id. at doc. 130 (email chain revealing efforts to develop talking points

for inter-agency meeting to discuss development of DIB Cyber Pilot, including recommendations regarding the classified status of the meeting, a proposed agenda, and draft talking points); id. at doc. 169 (email chain discussing and commenting on DOJ talking points regarding proposed amendments to the Homeland Security Act); id. at doc. 302 (email chain from DHS Director of Legislative Affairs to DHS program officials containing recommendations regarding how to respond to a request from a member of Congress for briefing on the DIB Cyber Pilot program).

As the Vaughn index demonstrates, agency stakeholders spent a significant amount of time communicating about the development and implementation of the DIB Cyber Pilot program. Because these communications reflect both inter and intra-agency deliberations on the advisability of particular courses of action related to myriad aspects of this complex cybersecurity program, Public Citizen, Inc. v. Office of Management and Budget, 598 F.3d 865, 875 (D.C. Cir. 2010), they are deliberative and properly withheld.

b. The Attorney-Client Privilege

The attorney-client privilege applies when a client communicates something to his or her lawyer with the intent that it remain confidential and for the purposes of securing "either (i) an opinion on law or (ii) legal services or (iii) assistance in some legal proceedings." In re Lindsey, 158 F.3d 1263, 1270 (D.C. Cir. 1998) (citing In re Sealed Case, 737 F.2d 94, 98-99 (D.C. Cir. 1984)). The privilege also encompasses any opinions given by an attorney to his client based upon facts communicated by the client. See, e.g., Mead Data Central, Inc. v. U.S. Dep't of the Air Force, 566 F.2d 242, 254 n.25 (D.C. Cir. 1977). In the FOIA context, the requirement that the attorney-client privilege involve confidential communications is satisfied if the communications suggest that "the government is dealing with its attorneys as would any private party seeking advice to protect personal interests. . . ." Coastal States Gas Corp. v. Dept. of Energy, 617 F.2d 854, 863 (D.C. Cir. 1980).

Because of the complex nature of the DIB Cyber Pilot, including the various legal issues implicated by its development and implementation, agency counsel within the various agency stakeholders often communicated with each other and their respective client agencies in order to address legal issues presented by the project. The withheld records fall generally into two interrelated groups: (1) legal papers, including memoranda and position papers, and (2) email communications containing legal analysis, advice, opinions and recommendations. See Tab A, ¶57; see also Tab C, ¶10. For example, DHS withheld in full three legal memoranda created by DOJ attorneys providing their analysis of legal issues related to the DIB Cyber Pilot. See Tab C, ¶¶12, 15; see also Tab B, at WIF doc. 20 (legal memoranda prepared by DOJ attorneys for DHS containing DOJ's legal research and analysis regarding the DIB cyber pilot). DHS also properly withheld talking points prepared by the Principal Deputy General Counsel within DOD for the Deputy Secretary of Defense that contain the PDGC's legal analysis of a potential legal issue raised with respect to the implementation of the DIB Cyber Pilot. Id. at WIF doc. 27. These legal memoranda and other documents prepared by agency counsel to advise their respective agency clients regarding legal issues related to the development and implementation of the DIB Cyber Pilot are properly withheld as protected under the attorney-client privilege. See Coastal States Gas Corp., 617 F.2d at 863 (exemption 5 applies when "the government is dealing with its attorneys as would any private party seeking advice to protect personal interests").

The same is true with respect to email communications containing the legal advice, opinions, and recommendations of the various agency counsel involved in analyzing the legal framework underpinning the DIB Cyber Pilot. As demonstrated by the Vaughn index, DHS properly applied Exemption 5 to, among other email communications containing the legal advice of agency counsel, an email chain among DHS counsel and program personnel regarding procurement issues in which DHS counsel provides legal analysis and comment regarding the

same. See Tab B, at doc. 305.; see also id. at doc. 372 (email chain among DOJ, DHS, and DOD counsel and program personnel at DHS and DOD containing counsels' advice regarding legal questions pertaining to the DIB Cyber Pilot; id. at doc. 373 (same); id. at doc. 381 (email chain containing DHS legal counsel's analysis and observations regarding a draft DIB evaluation document). Because these documents and email communications contain not only the agency stakeholders' requests for legal advice but also the legal opinion, advice, and recommendations of agency counsel regarding the establishment of the DIB Cyber Pilot, they were properly withheld as protected by the attorney-client privilege.

c. The Attorney Work Product Doctrine

DHS relied on the attorney work-product doctrine, in addition to the deliberative process privilege, to protect information contained within "Withheld in Full" documents numbered 15, 16, and 20 as well as the redacted portions of forty-five pages of e-mails Tab D, at ¶¶8, 9-113; see also Tab B, at 58. As shown in both the Vaughn index and the Declaration of Vanessa Brinkmann (Tab D), DHS, at the request of the Department of Justice, properly withheld in full the 2 legal memoranda and the legal position paper have been withheld in full because they contain the views and analysis of Department of Justice attorneys regarding the likelihood of possible legal challenges to certain aspects of the DIB Cyber Pilot as well as their views on possible litigation strategies to respond to the same. See Tab D, at ¶12. The same applies equally to the information redacted from the forty-five pages of emails that contain discussions reflecting the legal opinion and analysis of Department of Justice attorneys regarding their assessment of the likelihood of possible legal challenges to aspects of the DIB Cyber Pilot. Id. at ¶11-13.

Indeed, the attorney work-product doctrine prevents the disclosure of "documents prepared in anticipation of foreseeable litigation, even if no specific claim is contemplated."

Schiller, 964 F.2d at 1208. It applies so long as "some articulable claim, likely to lead to litigation" has arisen. Coastal States Gas Corp. v. Dep't of Energy, 617 F.2d 854, 865 (D.C. Cir. 1980). The doctrine thus protects information generated by legal counsel where "the document can fairly be said to have been prepared or obtained because of the prospect of litigation." In re Sealed Case, 146 F.3d 881, 884 (D.C. Cir. 1998) (citations omitted). In particular, the work-product doctrine also shields activities designed to forestall or prevent litigation. Thus, the Court of Appeals has noted:

> [i]t is often prior to the emergence of specific claims that lawyers are best equipped either to help clients avoid litigation or to strengthen available defenses should litigation occur. . . . If lawyers had to wait for specific claims to arise before their writings could enjoy work-product protection, they would not likely risk taking notes about such matters or communicating in writing with colleagues, thus severely limiting their ability to advise clients effectively. . . . Discouraging lawyers from engaging in the writing, note-taking, and communications so critical to effective legal thinking would . . . "demoraliz[e]" the legal profession, and "the interests of the clients and the cause of justice would be poorly served."

In re Sealed Case, 146 F.3d at 886 (quoting Hickman v. Taylor, 329 U.S. 495, 511 (1947)); see also Cities Serv. Co. v. Fed. Trade Comm'n, 627 F. Supp. 827, 832 (D.D.C. 1984) (documents that relate to "possible settlement discussions pertaining to foreseeable litigation are protected under the attorney work-product privilege").

As the Vaughn index demonstrates, DHS, at the request of DOJ, properly asserted the work product doctrine to withhold in full 2 legal memoranda prepared and a legal position paper by counsel at the Department of Justice analyzing whether a private party is an agent or instrument of the government for purposes of possible legal challenges to the DIB Cyber Pilot. See Tab B, at WIF docs. 15, 16; see also Tab D, at ¶¶11-14. The work product doctrine shields these particular documents from disclosure under FOIA in their entirety because these

documents contain analyses of the potential litigation risks associated with the Department of Justice's legal analysis of this issue and contains the views of the Department of Justice regarding potential defenses to any litigation that may ensue.

The same holds true with respect to information redacted from the forty-five pages of email communications referenced in the Brinkmann Declaration and the Vaughn index. These particular email communications contain the legal analysis, advice, and opinions of Department of Justice attorneys concerning the potential litigation risks associated with the development and implementation of the DIB Cyber Pilot and the government's defense of any litigation that may ensue. See, e.g., Tab B, at doc. 239 (email chain discussing DOJ's legal analysis regarding the participation of companies in the DIB Cyber Pilot and the potential litigation risks associated with the same). Because the legal advice and analysis discussed and referenced in these emails and the three legal documents were prepared by counsel at the Department of Justice to assess the government's litigation risk with respect to this highly sensitive cyber program, they were properly withheld under the work product doctrine.

5. DHS Properly Withheld Information Pursuant to Exemption 7

DHS withheld law enforcement materials pursuant to FOIA Exemption 7. Exemption 7 permits withholding of "records or information compiled for law enforcement purposes" meeting certain specified criteria. 5 U.S.C. § 552(b)(7). "In assessing whether records are compiled for law enforcement purposes, . . . the focus is on how and under what circumstances the requested files were compiled," and whether the files sought relate to anything that "can fairly be characterized" as relating to a law enforcement proceeding. Jefferson v. Dep't of Justice, 284 F.3d 172, 176–77 (D.C. Cir. 2002) (citations omitted). The range of law enforcement purposes falling within the scope of Exemption 7 includes government national security, homeland security, and counterterrorism activities. See, e.g., Ctr. for Nat'l Sec. Studies

v. U.S. Dep't of Justice, 331 F.3d 918, 926 (D.C. Cir. 2003); Gordon v. FBI, 388 F. Supp. 2d 1028, 1035-1036 (N.D. Cal. 2005) (recognizing that law enforcement threshold met by memoranda and e-mail messages created by FBI in its handling of various aviation "watch lists" created to "protect the American flying public from terrorists"); Coastal Delivery v. United States Customs Service, 272 F. Supp. 2d at 964-65 (reasoning that law enforcement requirement is satisfied by cargo-inspection data at seaports where disclosure could permit terrorists to direct activities to "vulnerable ports"). Furthermore, the DHS mission includes securing the homeland and law enforcement, and NPPD, the component within the Department with primary responsibility for the DIB Cyber Pilot,has a clear national security, homeland security and counterterrorism mission; thus DHS is entitled to deference when it identifies material as having been compiled for law enforcement purposes under Exemption 7. See Campbell v. U.S. Dep't of Justice, 164 F.3d 20, 32 (D.C. Cir. 1999).

The records at issue in this litigation were compiled for law enforcement purposes within the meaning of Exemption 7, because, as explained in the Holzer declaration, Herrington declaration, and Vaughn index, the records responsive to the plaintiffs' requests concern the creation and implementation of a cybersecurity pilot program, and this program was initiated o strengthen aspects of the national infrastructure that are vulnerable to attach by both foreign and domestic entities seeking to disrupt communications and information systems. See, e.g., Tab A ¶ ___. Accordingly, the records at issue in this litigation meet the threshold requirement for application of Exemption 7.

a. Exemption 7(d)

Law enforcement sources are entitled to the protection of 5 U.S.C. § 552(b)(7)(D), which permits the withholding or redacting of law enforcement records the release of which "could reasonably be expected to disclose the identity of a confidential source . . . and, in the case of a

record or information compiled by a criminal law enforcement authority in the course of a criminal investigation . . . information furnished by a confidential source." Exemption 7(D) requires no balancing of public and private interests. See Dow Jones & Co., Inc. v. Dept. of Justice, 917 F.2d 571, 575-76 (D.C. Cir. 1990). The exemption applies if the agency establishes that a source has provided information under either an express or implied promise of confidentiality. See Williams v. FBI, 69 F.3d 1155, 1159 (D.C. Cir. 1995). A confidential source is one who "provided information under an express assurance of confidentiality or in circumstances from which such an assurance could be reasonably inferred." U.S. Dept. of Justice v. Landano, 508 U.S. 165, 172 (1993) (internal quotation and citation omitted).

Here, as the Herrington declaration and Vaughn index explain, the DIB companies served as confidential sources of law enforcement information. DIB companies participating in the DIB Cyber Pilot shared cyber-incident data with DoD, including samples of malicious code that the companies found in their networks. Tab C ¶14. That information was then used by DoD to alert participating companies and the federal government as to signatures of the capture malware, to protect the networks of the defense industrial base and the federal government. The DIB companies participated with an express promise of confidentiality. Id.

b. Exemption 7(e)

DHS withheld operational methods, security procedures, technical vulnerability information, and countermeasure capabilities and techniques pursuant to Exemption 7(E). Exemption 7(E) permits withholding of information compiled for law enforcement purposes if release of the information "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E). The protection afforded by Exemption 7(E) is categorical for

information related to law enforcement techniques. See Smith v. Bureau of Alcohol, Tobacco and Firearms, 977 F. Supp. 496, 501 (D.D.C. 1997); Fisher v. Dept. of Justice, 772 F. Supp. 7, 12 n. 9 (D.D.C. 1991), aff'd, 968 F.2d 92 (D.C. Cir. 1992). Even if a law enforcement technique itself has been disclosed, but the public is not generally aware of the manner and circumstances in which the technique is employed, or the specific methods used by the particular agency, Exemption 7(E) still applies. See, e.g., Blanton, 63 F. Supp. 2d at 49-50; Coleman v. Federal Bureau of Investigation, 13 F. Supp. 2d 75, 83-84 (D.D.C. 1998). In some cases, even commonly known procedures have been protected from disclosure when "circumstances of their usefulness . . . may not be widely known," Wickline v. FBI, 1994 WL 549756, *5 (D.D.C. 1994), or when their use "in concert with other elements of an investigation and in their totality directed toward a specific investigative goal [] constitute a 'technique' which merits protection to ensure it future effectiveness." D'Alessandro v. U.S. Dept. of Justice, 1991 WL 35519, *4 (D.D.C. 1991) (citation omitted). It is sometimes not possible to describe a technique, even in very general terms, without disclosing the very information being withheld. See, e.g., Smith, 977 F. Supp. at 501.

Exemption 7(E) permits the withholding of information relating to national security activities when release of the information could help criminals evade detection. See, e.g., Tax Analysts v. IRS, 294 F.3d 71, 79 (D.C. Cir. 2002) ("It is clear that, under . . . Exemption 7, an agency may seek to block the disclosure of internal agency materials relating to guidelines, techniques, sources, and procedures for law enforcement investigations and prosecutions, even when the materials have not been compiled in the course of a specific investigation.").

As explained in the Holzer declaration, knowledge of the information withheld under 7(e) by DHS, including operational methods, security procedures, technical vulnerability information, and countermeasure capabilities and techniques, would enable individuals involved in criminal

or cyber-terrorist activities to adapt their activities and methods to penetrate cyber vulnerabilities or avoid detection. See Tab A ¶¶ 69-74. Furthermore, as explained above, disclosure of technical details pertaining to the DIB Cyber Pilot could facilitate unauthorized intrusions into DIB company or the government's networks or interference with future cybersecurity programs developed based on the DIB Cyber Pilot. See id. In sum, the information would disclose cyber security techniques and procedures, and would allow individuals to detect and target vulnerabilities within the DIB sector, DHS properly withheld this information under (b)(7)(E).

CONCLUSION

For the foregoing reasons, the Court should enter summary judgment for defendant DHS.

Dated: August 30, 2013

Respectfully submitted,

STUART F. DELERY
Assistant Attorney General

JOHN R. TYLER
Assistant Director

/s/ Lisa Zeidner Marcus

LISA ZEIDNER MARCUS
TAMRA T. MOORE
Trial Attorneys
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, 7th Floor
Washington, DC 20001
Tel: (202) 514-3336
Fax: (202) 616-8460
E-mail: lisa.marcus@usdoj.gov

Counsel for Defendant