IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER Plaintiff, v. THE UNITED STATES DEPARTMENT OF HOMELAND SECURITY Defendant.	)	No. 1:12-cv-00333-GK

PLAINTIFF'S MEMORANDUM OF POINTS AND AUTHORITIES IN OPPOSITION TO DEFENDANT'S MOTION FOR SUMMARY JUDGMENT AND IN SUPPORT OF PLAINTIFF'S CROSS-MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

EXHIBITS

INTRODUCTION

Plaintiff the Electronic Privacy Information Center ("EPIC") opposes Defendant U.S. Department of Homeland Security's ("DHS") August 30, 2013 Motion for Summary Judgment, and cross-moves for summary judgment in favor of EPIC.

EPIC challenges the DHS' withholding of documents, in full and in part, related to EPIC's Freedom of Information Act ("FOIA") requests seeking records concerning the Defense Industrial Base ("DIB") Cyber Pilot to monitor defense contractor computer networks. The program was conducted in conjunction with the U.S. Department of Defense ("DoD"). Specifically, EPIC Challenges:

1. DHS' failure to conduct a reasonable search for responsive documents;
2. DHS' failure to establish that documents have been properly classified;
3. DHS' failure to establish that redacted information falls within the scope of a specified statutory exemption;
4. DHS' improper application of Exemption 4 to withhold non-private information;
5. DHS' improper withholding of information under Exemption 5 that does not qualify as an "Inter-agency or Intra-agency Memorandum[] or Letter";
6. DHS' failure to establish that information withheld under Exemption 7(D) was furnished by Corporate entities acting as a "confidential source";
7. DHS' invocation of Exemptions for which there is no explanation.

FACTUAL BACKGROUND

This Motion for Summary Judgment concerns EPIC's Freedom of Information Act ("FOIA") Request for information about the government's collection of the private communications of Internet users and compliance with federal privacy law.

I. The Defense Industrial Base Cyber Pilot

In May 2011, the Department of Homeland Security ("DHS") and the National Security Agency ("NSA") undertook the "DIB Cyber Pilot" to monitor Internet traffic flowing through certain Internet Service Providers ("ISPs") from Internet users to a select number of defense contractors. The program was confirmed by Deputy Defense Secretary William J. Lynn III in a speech on June 16, 2011. Lynn explained that the government would provide threat intelligence to certain companies to help identify and stop malicious activity within their networks. Other National Security Agency ("NSA") officials stated that the Agency could monitor network communications and identify suspicious network behavior. However, the Washington Post reported that the Department of Justice ("DOJ") expressed concern that the DIB Cyber Pilot program could "run afoul of laws forbidding government surveillance of private Internet traffic." EPIC sought records to determine whether in fact the DIB Cyber Pilot program complied with federal wiretap laws, including the Electronic Communications Privacy Act. *See* 18 U.S.C. §§ 2510 *et. seq.* (2013).

The reports identified participating ISPs to include AT&T, Verizon, and Century Link, and defense contractors to include Lockheed Martin, CSC, SAIC, and Northrop Grumman. The DoD announced on May 11, 2012 that the one-year DIB Pilot Program had concluded and the program would be fully implemented and expanded to include DIB Enhanced Cybersecurity Services.

II. EPIC's FOIA Request

On July 26, 2011, EPIC filed a FOIA request with DHS ("EPIC's FOIA Request"), including a request for news media fee status and for a fee waiver. Specifically, EPIC's FOIA Request sought the following five (5) categories of documents:

1. All contracts and communications with Lockheed Martin, CSC, SAIC, Northrop Grumman or any other defense contractors regarding the new NSA pilot program;

2. All contracts and communications with AT&T, Verizon and CenturyLink or any other IPSs regarding the new NSA pilot program;

3. All analyses, legal memoranda, and related records regarding the new NSA pilot program;

4. Any memoranda of understanding between NSA and DHS or any other government agencies or corporations regarding the new NSA pilot program;

5. Any privacy impact assessment performed as part of the development of the new NSA pilot program.

By letter dated August 3, 2011, DHS acknowledged receipt of EPIC's FOIA Request and notified EPIC that no responsive documents had been located for category 5. DHS then referred EPIC's FOIA Request to the National Protection and Programs Directorate ("NPPD"), a DHS component, for further processing of the remaining four categories of documents. NPPD failed to provide even an acknowledgement of the receipt of EPIC's FOIA Request. Accordingly, on January 5, 2011, more than 100 days after DHS' initial response, EPIC transmitted an administrative appeal alleging that the Agency had missed its statutory deadlines in regard to categories 1-4 of EPIC's FOIA Request. On January 23, 2012 a FOIA Agent in NPPD contacted EPIC attorney Amie L. Stepanovich by telephone and indicated that the component would "start processing" EPIC's FOIA Request. However, EPIC received no further communications from NPPD.

III. EPIC's Complaint and Subsequent Activity

Almost 40 days after the submission of the administrative appeal, EPIC filed a complaint in federal district court on March 1, 2012. The complaint alleged that DHS failed to comply with the statutory provisions of the FOIA. DHS filed an answer on May 1, 2012.

On August 31, 2012, the Parties agreed to narrow the scope of EPIC's FOIA Request. EPIC agreed to exclude draft documents from the scope of the request, and narrowed the categories of documents requested as follows:

1. All contracts and communications with Lockheed Martin, CSC, SAIC, Northrop Grumman or any other defense contractors regarding the DIB Cyber Pilot;

2. All contracts and communications with AT&T, Verizon and CenturyLink or any other IPSs regarding the DIB Cyber Pilot;

3. All legal and technical analyses, including legal memoranda, regarding the DIB Cyber Pilot;

4. Any memoranda of understanding between NSA and DHS or any other government agencies or corporations regarding the DIB Cyber Pilot.

After numerous delays and extensions, DHS produced approximately 1,300 pages of partially-redacted documents on April 15, 2013. A partial preliminary Vaughn Index was provided on June 15, 2013. The remaining preliminary Vaughn Index was provided on June 22, 2013. In response to questions raised by EPIC, DHS made a supplemental production of documents on August 16, 2013. DHS' Motion for Summary Judgment was filed in this Court on August 30, 2013. Dkt. Nos. 53-56 ("DHS Motion"). DHS' Motion included three declarations from government officials as Exhibits three, five, and seven. ("Second Holzer Decl.," "Herrington Decl.," and "Brinkmann Decl." respectively). DHS' Motion also included the final version of the Agency's Vaughn Index as Exhibit 4. ("Vaughn Index"). EPIC now responds.

STANDARD OF REVIEW

Summary judgment is appropriate when there is no genuine issue as to the material facts, and the moving party demonstrates it is entitled to judgment as a matter of law. Fed. R. Civ. P. 56; *Diamond v. Atwood*, 43 F.3d 1538, 1540 (D.C. Cir. 1995). FOIA lawsuits are typically resolved on cross-motions for summary judgment. *Taitz v. Astrue*, 806 F. Supp. 2d 214, 217

(D.D.C. 2011), *citing Reliant Energy Power Generation v. FERC*, 520 F. Supp. 2d 194, 200 (D.D.C. 2007). A court reviews agency handling of a FOIA request *de novo*. 5 U.S.C. § 552(a)(4)(B).

The U.S. Supreme Court "repeatedly has stressed the fundamental principle of public access to Government documents that animates the FOIA." *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 151-52 (1989). "In enacting FOIA, Congress struck the balance it thought right--generally favoring disclosure, subject only to a handful of specified exemptions--and did so across the length and breadth of the Federal Government." *Milner v. Dep't of the Navy*, 131 S. Ct. 1259, 1266 (2011). As the Court has previously explained, "[t]he basic purpose of FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed." *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978). The FOIA's "basic purpose reflect[s] a general philosophy of full agency disclosure unless information is exempted under clearly delineated statutory language." *U.S. Dept. of Air Force v. Rose*, 425 U.S. 352, 360-61 (1976), quoting S. Rep. No. 813, 89th Cong., 1st Sess., 3 (1965). FOIA was meant to be a "disclosure statute," not a "withholding statute." *Milner*, 131 S. Ct. at 1262. The FOIA "mandates a strong presumption in favor of disclosure." *EPIC v. Dep't of Justice*, 511 F. Supp. 2d 56, 64 (D.D.C. 2007) (internal citations omitted).

The FOIA includes exemptions from disclosure, "[b]ut these limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act." *Rose*, 425 U.S. at 361. Therefore FOIA exemptions "must be narrowly construed." *Id*. "The statute's goal is broad disclosure, and the exemptions must be given a narrow compass." *Milner*, 131 S. Ct. at 1261 (internal citations omitted). Furthermore, "the burden is on the agency to sustain its

action." 5 U.S.C. § 552(a)(4)(B); *see also EPIC v. Dept. of Homeland Security*, 384 F. Supp. 2d 100, 106 (D.D.C. 2005).

ARGUMENT

As set forth below, DHS did not conduct a sufficient search for documents responsive to EPIC's FOIA Request. Furthermore, DHS asserted improper exemptions to withhold information that must be disclosed to EPIC and to the public. Finally, DHS asserted exemptions without any justification for those exemptions. Accordingly, EPIC respectfully requests the Court to order DHS to conduct a further search for documents, using information provided by EPIC as a guide as this Circuit has instructed, and to disclose records that were improperly withheld.

I. DHS Did Not Conduct A Sufficient Search for Documents Responsive to EPIC's FOIA Request

The government "must show beyond material doubt [] that it has 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 order to conduct such a search, the government must "follow through on obvious leads to discover requested documents," *Campbell v. U.S. Dep't of Justice*, 164 F.3d 20, 28 (D.C. Cir. 1998), and "cannot limit its search" to only one or more places if there are additional sources "that are likely to turn up the information requested." *Oglesby v. U.S. Dep't of Army*, 920 F.2d 57, 68 (D.C. Cir. 1990). Although "[a]n agency has discretion to conduct a standard search in response to a general request, [] it must revise its assessment of what is 'reasonable' in a particular case to account for leads that emerge during its inquiry." *Campbell v. U.S. Dep't of Justice*, 164 F.3d 20, 28 (D.C. Cir. 1998). "Consequently, the court evaluates the reasonableness of an agency's search based on what the agency knew at its conclusion rather than what the agency speculated at its inception. *Id.* Summary judgment is inappropriate if the government's declarations "raise serious doubts as to the completeness of the

search or are for some other reason unsatisfactory," *Perry v. Block*, 684 F.2d 121, 127 (D.C. Cir. 1982), or if there are "positive indications of overlooked materials," *Founding Church of Scientology v. NSA*, 610 F.2d 824, 837 (D.C. Cir. 1979).

DHS failed to perform a sufficient search for documents responsive to EPIC's request in light of what was revealed by the documents DHS did produce. The documents DHS did find to be responsive to EPIC's request clearly indicate an insufficient search for responsive documents. As Exhibit 4 demonstrates, there are numerous potentially responsive documents either referenced in or attached to documents produced to EPIC. For example, two attachments to an email chain with the subject "Cybersecurity and NSS" – one attachment labeled "Privacy Oversight.DHS task_20111214.docx" and the other labeled "Privacy Oversight.taskdiv.docx." *See* Exhibit 4-1 at Bates page 226-31. Another email chain with the subject "Updated POA&M for DIB Pilot" includes an attached document labeled "JCSS POAM 18Nov11nmd.docx. *See* Exhibit 4-3 at Bates pages 703-04. Presumably this document discusses the "plan of action and milestones ("POAM") for the DIB Pilot. In an email with the subject "JCSP Transition Activities" it explicitly says, "Please find attached the final briefing and meeting agenda for tomorrow's CIO/CISO meeting." Exhibit 4-4 at Bates page 811. Attached to this email is one document labeled "CIO-CISO JCSP Meeting Agenda_FINAL_12132011.doc" and another document labeled "JCSP Briefing to CIO and CISOs (FINAL)(13Dec11).ppt." *Id.*

These documents, or the final versions of these documents, are likely responsive and should have been reviewed for potential production to EPIC. The government's "page-by-page and line-by-line reviews of the potentially responsive documents" gave the government thorough knowledge of and clear leads to additional responsive documents not represented in its insufficient search. *See* Second Holzer Decl. at ¶ 44.

Furthermore, EPIC previously pointed out to DHS that potentially responsive documents were referenced and/or attached in the emails produced to EPIC. *See* Second Holzer Decl. at ¶¶ 47-48. On June 20, 2013, EPIC sent DHS "a partial list of bates page numbers that [were] examples of documents that reference attachments" that were potentially responsive to EPIC's request. *See* Third Stepanovich Decl. at ¶ 16; *see also* Exhibit 3-D. The partial list of Bates page numbers was provided by EPIC as an example to help guide the government's re-evaluation of the sufficiency of its search. The sixteen Bates page numbers provided resulted in the review of seventeen additional documents and the production of five additional documents to EPIC. *See* Second Holzer Decl. at ¶ 48.

According to the government, it performed a supplemental search in light of the examples provided by EPIC of potentially responsive documents being either referenced or attached to emails produced to EPIC. Second Holzer Decl. at ¶ 47-48. Despite the supplemental search, the government only found and reviewed the potentially responsive documents referenced or attached to the email documents cited by EPIC as examples. *Id.* The indications of potentially responsive documents occur throughout the production provided to EPIC. Exhibit 4 provides an exhaustive list of produced documents that reference potentially responsive documents and/or have potentially responsive documents as attachments.

The government failed to appropriately revise its assessment of what constituted a reasonable search in light of clear indicators that its search was insufficient. "[I]f, in the face of well-defined requests and positive indications of overlooked materials, an agency can so easily avoid adversary scrutiny of its search techniques, the Act will inevitably become nugatory." *Founding Church of Scientology v. NSA*, 610 F.2d 824, 837 (D.C. Cir. 1979). As such, DHS' search was insufficient as a matter of law.

II. DHS Has Not Presented Adequate Evidence to Establish that Information Responsive to EPIC's FOIA Request Is Properly Classified by Designated Classification Authorities

Defendant's Motion argues that certain information is properly classified and therefore exempt from disclosure pursuant to Exemption 1. DHS Motion at 18-23. However, DHS has not established that these records are properly classified. Therefore, DHS' Exemption 1 claim cannot support its withholding of these records.

A. DHS Has Not Established that David J. Sherman Has Classification Authority Under Executive Order 13526 or its Predecessor

To properly invoke FOIA Exemption 1, the "government must demonstrate that information is in fact properly classified pursuant to both procedural and substantive criteria." S. Rep. No. 93-100, at 6 (1974) (Conf. Rep.); *see also Goldberg v. Dept. of State*, 818 F.2d 71, 77 (D.C. Cir. 1987), *cert denied*, 485 U.S. 904 (1988); *Lesar v. Dept. of Justice*, 636 F.2d 472, 483 (D.C. Cir. 1980); *Allen v. CIA*, 636 F.2d 1287, 1291 (D.C. Cir. 1980). The current standard for classification is embodied in Executive Order 13526.[1] Executive Order 13526 prescribes "a uniform system for classifying, safeguarding, and declassifying national security information…" Executive Order 13526. "If there is significant doubt about the need to classify information, it shall not be classified." *Id*. at Section 1.1(b).

Information may only be deemed "classified" if each of the following conditions are met:

(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 [provided by the Executive 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,

[1] As explained by DHS, "two Executive Orders contain[ing] nearly identical requirements for originally classifying information under the terms of their orders, and substantially similar categories of information eligible for classification consideration" were in effect during the creation of relevant Agency records. DHS Motion at 20. For similar reasons to those described by DHS, EPIC discusses the most recent Executive Order. *Id*. at 19-20.

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

Exec. Order 13256, Section 1.1(a). Under Executive Order 13256, only the following officials have the authority to classify information:

> (5) the President and the Vice President;
> (6) agency heads and officials designated by the President; and
> (7) United States Government officials delegated this authority pursuant to paragraph (c) of this section.

Executive Order 13526, Section 1.3 (a). The Executive Order gives specific instructions on the issue of delegation of classification authority:

> (1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.
> (2) "Top Secret" original classification authority may be delegated only by the President, the Vice President, or an agency head or official designated pursuant to paragraph (a)(2) of this section.
> (3) "Secret" or "Confidential" original classification authority may be delegated only by the President, the Vice President, an agency head or official designated pursuant to paragraph (a)(2) of this section, or the senior agency official designated under section 5.4(d) of this order, provided that official has been delegated "Top Secret" original classification authority by the agency head.
> (4) Each delegation of original classification authority *shall be in writing* and the *authority shall not be redelegated* except as provided in this order. Each delegation shall identify the official by name or position.
> (5) Delegations of original classification authority shall be reported or made available by name or position to the Director of the Information Security Oversight Office.

Executive Order 13526, Section 1.3(c) (emphasis added).

DHS argues that sections of eighteen partially produced records and the full text of six withheld in full records are properly classified because David J. Sherman, Associate Director for Policy and Records at the NSA has original classification authority pursuant to Executive Order 13526. However, the NSA has not presented adequate evidence to establish that Mr. Sherman has been delegated original classification authority.

While an Agency may submit a declaration to provide evidence for a claimed exemption, such an affidavit must "forge the logical connection between the information withheld and the claimed exemption." *Oglesby v. U.S. Dept. of Army*, 79 F.3d 1172, 1178 (D.C. Cir. 1996) (internal citations omitted). Mr. Sherman did not submit his own declaration. The second declaration of James V.M.L. Holzer states, "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." Second Holzer Decl. ¶ 55 (emphasis in original). This language is mirrored in DHS' Motion for Summary Judgment. DHS Motion at 21 ("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."). Mr. Holzer does not offer any basis to support his claim of Mr. Sherman's alleged classification authority. DHS presents no evidence that Mr. Sherman has been delegated classification authority by the President or Vice President, or an agency head that was first delegated such authority by the President or Vice President, nor does Mr. Holzer represent that he has personal knowledge of Mr. Sherman's alleged classification authority. *See Weisberg v. Dept. of Justice*, 628 F.2d 365 (D.C. Cir. 1980) (holding a declaration impermissible where the declarant had no personal knowledge of the information asserted).

Accordingly, DHS has not met its burden of proof on the assertion that documents responsive to EPIC's FOIA Request are properly classified pursuant to Executive Order 13256 or its predecessor. 5 U.S.C. § 552(a)(4)(B); *see also EPIC v. Dept. of Homeland Security*, 384 F. Supp. 2d 100, 106 (D.D.C. 2005) ("the burden is on the agency to sustain its action."). Mr. Holzer failed to establish that Mr. Harrington has been delegated classification authority in order to determine that documents are properly classified as required by Exemption 1.

III. DHS Has Not Established that Information Responsive to EPIC's FOIA Request Is Properly Exempt from Disclosure Pursuant to Exemption 3

DHS had redacted information in nineteen partially-withheld documents and one withheld-in-full document under Exemption 3. DHS Motion at 24-27; Vaughn Index at 193-207. Exemption 3 permits agencies to withhold information that is "specifically exempted from disclosure" by another federal statute "if that statute – establishes particular criteria for withholding the information or refers to the particular type of material to be withheld." 5 U.S.C. § 552(b)(3). DHS invoked two federal statutes to withhold information – Section 6 of the National Security Act of 1959, Pub. L. No. 86-36, 73 Stat. 63 (codified at 50 U.S.C. § 3605) ("Section 6") and 18 U.S.C. § 798 (2013) ("Section 798").

Under Exemption 3, the relevant inquiries for the Court are (1) if a particular statute qualifies as an exempting statute and (2) if the information falls within the statutes' coverage. *Goland v. CIA*, 607 F.2d 339, 350 (D.C. Cir. 1978). EPIC does not dispute here that Section 6 and Section 798 are Exemption 3 statutes for the purpose of FOIA. *See Founding Church of Scientology of Washington, D.C. v. NSA*, 610 F.2d 824, 828 (D.C. Cir. 1979); *Larson v. Dept. of State*, 565 F.3d 857, 868 (D.C. Cir. 2009). However, DHS has failed to provide sufficient evidence that the information sought by EPIC falls within the scope of either statute

A. DHS Has Not Established that Documents Are Properly Classified Under Section 798

DHS invokes Section 798 to withhold information pursuant to Exemption 3. Section 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." 18 U.S.C. § 798 (2013). Section 798 applies only to records that contain "classified information."

Insofar as the Court holds that documents described in Section II are not properly classified, the records are not within the scope of Section 798 and therefore may not be withheld under Exemption 3.

B. DHS Has Not Met Its Burden of Proof to Establish that Documents are Related to NSA's "Functions or Activities" Under Section 6

DHS has not provided adequate information to justify withholding information pursuant to Section 6. In relevant part, Section 6 provides:

> [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, of any information with respect to the activities thereof, or of the names, titles, salaries, or number of persons employed by such agency."

50 U.S.C. § 3605. By the explicit terms of Section 6, withheld information must relate to the functions or activities *of the National Security Agency* – not another Agency or non-governmental entity. *Id*.; *See also Larson v. Dept. of State*, 565 F.3d 857, 868 (D.C. Cir. 2009) ("the NSA…need only demonstrate that the withheld information relates to the organization of the NSA or any function or activities *of the agency*." (emphasis added)); *People for the American Way Foundation v. NSA/CSS*, 462. F. Supp. 2d 21, 31 (D.D.C. 2006) ("Whether the TSP, one of the NSA's many SIGINT programs involving the collection of electronic communications, is ultimately determined to be unlawful, its potential illegality cannot be used in this case to evade the 'unequivocal' language of Section 6, which 'prohibits the disclosure of information relating the *NSA's functions and activities*.'" (emphasis added)). The DIB Cyber Pilot was a joint venture between the NSA and DHS. DHS Motion at 2. DHS has not met its burden of proving that the withheld information relates solely to the functions or activities of the NSA.

The Vaughn Index entries for many documents are inadequate to demonstrate that withheld information relates specifically to the functions or activities of the NSA. For example,

in several documents DHS has partially withheld pursuant to Section 6 DHS' description of the information relates specifically to the activities of other government agencies, and not NSA:

- "This is an eight page email chain the summarizes the properly classified legal issues DOJ raised regarding the DIB Pilot." (Vaughn Index at 196, Document 438);
- "This is a two page email discussing questions and issues that warrant further discussion amongst the various agencies." (Vaughn Index at 197-198, Document 442).

Still other documents relate to the activities of private companies:

- "This is a three page email discussing the number of companies involved in the DIB pilot." (Vaughn Index at 197, Document 441);
- "This document discusses assessments of a company's implementation capabilities regarding technical capabilities and acceptable levels of security." (Vaughn Index at 207, Withheld-in-Full Document 5).

Further, in other cases, DHS' Vaughn Index "merely recite[s] statutory standards," but fails to state the Agency's factual basis for its response in the required level of detail. *See Larson v. Dept. of State*, 565 F.3d 857, 868 (D.C. Cir. 2009). The Vaughn Index entry for three documents does no more than reiterate the Section 6 statutory standard. *See* Vaughn Index at 193 (Document 433: "DHS asserted Exemption…3 …to protect the functions of NSA pursuant to Section 6 of the National Security Agency Act of 1959.); Vaughn Index at 195 (Document 437: "The document…is covered by P.L. 86-36…to protect the functions of NSA pursuant to Section 6 of the National Security Agency Act of 1959"); Vaughn Index at 204 (Document 454: "DHS asserted Exemption…3…to protect the functions of NSA pursuant to Section 6 of the National Security Agency Act of 1959.).

Finally, DHS in one instance fails to provide any explanation whatsoever for the redaction of certain information. The description of Document 434 explains that Section 6 was only invoked to withhold "special compartmented intelligence classification markings." However, within the twelve-page document, it is apparent that information beyond the

classification markings has been redacted under Section 6. *See* Exhibit 5. DHS has provided no justification for these redactions.

As DHS has not met its burden of proof to withhold information pursuant to Section 6, the information should be ordered released immediately.

IV. DHS Has Improperly Applied Exemption 4 to Withhold Information that Must be Disclosed

DHS misapplies the test under Exemption 4 in order to withhold information that should be properly disclosed. Exemption 4 specifically exempts from disclosure "trade secrets and commercial or financial information" that is "obtained from a person and privileged or confidential." 5 U.S.C. § 552(b)(4) (2013).[2]

A. DHS May Not Withhold Public Information Under Exemption 4

DHS largely invokes Exemption 4 to withhold the identities of the companies participating in the DIB Cyber Pilot. But the FOIA does not establish a right of privacy for companies. *See FCC v. AT&T*, 131 S. Ct. 1177 (2011). The non-private identities of well-known corporations do not fall within the scope of Exemption 4. Company names are not confidential commercial information within the meaning of Exemption 4. Further, in this case the names were not provided by a person, and instead were circulated between government employees.

1. DHS Cannot Withhold Information Under Exemption 4 That Was Not "Obtained From a Person"

The identity of a corporation within the documents at issue cannot be said to have been "obtained from a person" within the meaning of Exemption 4. "Information may be 'obtained from a person' if provided by individuals, corporations, or numerous other entities, but not if it was generated by the federal government." *Comptel*, 910 F. Supp. 2d at 115, *citing Bd. Of Trade*

[2] DHS makes no attempt to argue that the information withheld is a "trade secret," nor that it is either "financial" or "privileged." Accordingly, EPIC does not address those arguments here.

v. CFTC, 627 F.2d 392 (D.C. Cir. 1980); *See also Fisher v. Renegotiation Bd.*, 355 F. Supp. 1171, 1174 (D.D.C. 1973) ("Exemption 4 was construed 'to encompass only information received from persons outside the Government'."). Information generated by the government may only be protected if it "summarize[s] information obtained by another person." *Comptel*, 910 F. Supp. 2d at 115, *citing Gulf & W. Indus. v. U.S.*, 615 F.2d 527, 529-30 (D.C. Cir. 1979).

Of the thirteen partially redacted and nine withheld-in-full documents that invoke Exemption 4, the vast majority of them are emails between DHS staff. *See, e.g.,* Vaughn Index at 11, Document 22; Vaughn Index at 44, Document 90; Vaughn Index at 49, Document 100; Vaughn Index at 55, Document 110; Vaughn Index at 144, Document 306; Vaughn Index at 180, Document 404. References to corporate identities within those emails were obviously not received from a person outside of DHS, nor do they summarize such information. *See Comptel*, 910 F. Supp. 2d at 116 ("the FCC has not alleged that the information was 'obtained from a person.' For example, the name of an SBC staffer in an email sent from FCC staff to SBC staff would not likely constitute information 'obtained from a person.'"). DHS provides no argument as to why the Agency believes that the corporate identifiers should be considered as "obtained by a person," and therefore it is impossible to guess upon its rationale. The information should not have been redacted.

2. Public Information is Not "Commercial Information" For Purposes of Exemption 4

Under Exemption 4, a government agency may redact certain information if it is either a "trade secret" or "commercial or financial." 5 U.S.C. § 552(b)(4). "Commercial information need not be limited to information that 'reveals basic commercial operations,' but may include any information in which the submitter has a 'commercial interest.'" *See Comptel v. FCC*, 910 F. Supp. 2d 100, 115 (D.D.C. 2012), *citing Pub. Citizen Health Research Grp. v. FDA*, 704 F.2d

1280, 1290 (D.C. Cir. 1983). Within the FOIA, "commercial information" is given its ordinary meaning and is to be construed broadly. *See Comptel*, 910 F. Supp. 2d at 115, *citing Nat'l Ass'n of Home Builders v. Norton*, 309 F.3d 26, 28 (D.C. Cir. 2002) (quotations omitted). This Court has previously explained, "business sales statistics, research data, overhead and operating costs, and financial conditions" may fall within the scope of "commercial information." *See*, *Comptel*, 910 F. Supp. 2d at 115-16. However, the definition is not all-encompassing. *See Id.*, *citing Chi. Tribune v. FAA*, 1998 WL 242611 (N.D.Ill. 1998) (holding that information is not commercial simply because it concerns events that occurred during revenue-producing operations). This Court has previously held that the identities of corporations were not exempt from disclosure under Exemption 4. *See Hodes v. U.S. Dept. of Housing and Urban Devlpmt*, 532 F. Supp. 2d 108 (D.D.C. 2008); *see also Comptel*, 910 F. Supp. 2d at 115-16 (holding that the names of some corporate employees did not fall within the definition of commercial information).[3]

In this case, the identity of companies involved in the DIB Cyber Pilot is not commercial information. While the identity of a corporation may figure in corporate transactions, it is not information in which a company can be said to have a "commercial interest."

Notably, DHS does not argue that the redacted information itself is commercial. Rather, DHS asserts that companies provided the information for commercial reasons that may hypothetically implicate "financial stakes," specifically (1) that a company "*could* face increased cyber targeting" and (2) "*could* be viewed as an admission of cyber vulnerability." DHS Motion at 28 (emphasis added).[4] The Herrington Declaration offers similar speculation. *See* Herrington

[3] DHS also redacts employee emails under Exemption 4. To the extent that these were redacted specifically to shield the name of the corporate entity, the same arguments would apply.

[4] This case raises issues comparable to those in *Sears, Roebuck & Co. v. GSA*, 384 F. Supp. 996 (D.D.C. 1974). In *Sears*, a reverse-FOIA case, Plaintiff Sears, Roebuck & Co. sought to enjoin the disclosure of certain documents the company had submitted to the government pursuant to Executive Order. In arguing that the information should not be disclosed, Sears asserted that "disclosed [would] adversely affect the goodwill of Sears and further present opportunities for adverse publicity and unwarranted litigation." *Id*. at 1007. However, the Court found that argument

Decl. at ¶ 11 ("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…" (emphasis added)). This is a vast departure from the standard that has been adopted by this Court. Indeed, it is hard to imagine an occasion when information provided to the government by a corporation does not implicate some commercial interest, even when, as here, the information is not commercial. Additionally, as DHS concedes, in many cases the identity of the participating company was not withheld. Second Holzer Decl. at ¶ 64 ("Generally speaking, DHS did not withhold the identities of the CSPs on an Exemption 4"). Obviously, at least two participating companies (AT&T and Century Link) did not believe that their participation implicated a commercial interest. *See Hodes*, 532 F. Supp. 2d at 118 ("[the defendant] does not demonstrate with specificity that substantial competitive harm…would result from disclosure when only a small subset of commercial entities would be affected and they might prefer to receive their funds in exchange for losing anonymity.").

For the reasons set forth above, the non-private identities of corporations cannot be "commercial information" within the meaning of Exemption 4.

3. Public Information is Not "Confidential" Under Any Exemption 4 Standard

For many of the same reasons that the corporate names are not commercial information, the identifying information is not "confidential." To determine if *private* information is confidential this Court applies one of two tests, depending on the circumstances under which the information was disclosed. *See* DHS Motion at 27-28 (emphasis added). If information was

---

unpersuasive, "this fear of potential loss of goodwill is tenuous at best…it is just as likely that evidence of Sears' compliance…will enhance, not diminish Sears' corporate image." *Id*. Similarly, evidence of corporate participation in the DIB Cyber Pilot is likely to be perceived as positive reinforcement for corporate cybersecurity practices. As DHS points out, "according to a 2012 study…the average annualized cost of cybercrime for defense industry companies in 2012 was $21.7 million." DHS Motion at 28. Companies taking additional steps to protection their networks are more likely to be seen as a deterrent to a potential cybercriminal.

disclosed voluntarily, it is considered confidential 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 Commission*, 975 F.2d 871, 879 (D.C. Cir. 1992). However, information that is disclosed under duress must meet a more stringent test for confidentiality, namely that disclosure would "impair the Government's ability to obtain necessary information in the future or . . . cause substantial harm to the competitive position of the person from whom the information was obtained." *Nat'l Parks and Conservation Ass'n v. Morton*, 498 F.2d 765, 770 (D.C. Cir. 1974).

As an initial matter, before one of the tests for confidentiality can be invoked, information must necessarily be deemed "private." *See* DHS Motion at 27 (discussing how both tests for confidentiality of documents apply to "private commercial information"); *see also* Herrington Decl. at ¶ 8 ("Pursuant to established procedures and applicable regulations, the Government will protect *sensitive nonpublic information* under this Program…" (emphasis added)). The publicly recognized identities of corporations are, by definition, not private at all, but widely known, public information. Just as DHS does not argue that the withheld information is commercial on its own, the Agency also does not assert that it is confidential, only that its use in this context would reveal private activities of a corporation. *See* DHS Motion at 28-29.

Agency employees were aware of the identities of defense contractors prior to the initiation of the DIB Cyber Pilot.[5] Accordingly, it is difficult to determine at what point in the transaction to become a participant in the DIB Cyber Pilot the corporate name was officially submitted to DHS in order to determine if that transaction was voluntary or compulsory. While

[5] "Contracts valued at $6.5 million or more are announced each business day at 5 p.m. Contract announcements issued within the past 30 days are listed below. Older contract announcements are available from the contract archive page. Contract announcements are also available by e-mail subscription." Contract, U.S. Department of Defense (last visited Sept. 25, 2013), *available at* http://www.defense.gov/contracts/default.aspx.

participation in the DIB Cyber Pilot may have been on a voluntary basis, once a company chose to participate, the company would have been compelled to identify itself to the government. *See Madison Mechanical, Inc. v. NASA*, 2003 WL 1477014 at *4 ("submission of this information is a mandatory prerequisite to selection for the contracts."). Therefore, the corporate identities should be evaluated under the second, more stringent test for confidential information.

As previously explained, information which is compelled from a company is "confidential" if its revelation would "impair the Government's ability to obtain necessary information in the future or . . . cause substantial harm to the competitive position of the person from whom the information was obtained." *Nat'l Parks and Conservation Assn.*, 498 F.2d at 770.

Disclosure of a corporate identity is not likely to "impair the Government's ability to obtain necessary information in the future." *See Nat'l Parks and Conservation Assn.*, 498 F.2d at 765. Defense industry companies have a vested financial interest in having the most secure networks available. This serves as incentive for companies to participate in government cybersecurity programs, independent of promises of anonymity. As DHS points out, "according to a 2012 study . . . the average annualized cost of cybercrime for defense industry companies in 2012 was $21.7 million." DHS Motion at 28. It is clearly within the best interests of the contractors to take affirmative steps to protect their networks, and to advertise as much to their customers. One major defense contractor explains in its 2012 financial report, "if we are unable to protect sensitive information, our customers or governmental authorities could question the adequacy of our threat mitigation and detection processes and procedures." Lockheed Martin Corporation 2012 Annual Report (Lockheed Martin, 2012) at 15 ("Lockheed Martin Report").[6]

[6] *Available at* http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/2012-Annual-report.pdf.

Further, the disclosure will also not "cause substantial harm to the competitive position of the person from whom the information was obtained." *See Nat'l Parks and Conservation Assn.*, 498 F.2d at 765. Companies that identify as "defense contractors," and were therefore eligible to participate in the DIB Cyber Pilot derive a large majority of their profits from contracts with the U.S. Government. For example, in 2012 defense contractor Lockheed Martin identified $38,788,000,000, or 80%, in net sales to the U.S. Government, while only a fraction of that in combined sales to all other customers. *See* Lockheed Martin Report at 68.

DHS argues that the test for voluntarily supplied information should apply to determine the confidentiality of the corporate identifiers because "participation by DIB companies and [Commercial Service Providers] in the DIC [sic] Cyber Pilot was voluntary, and the information provided by these companies to the government was also done on a voluntary basis." DHS Motion at 28. As explained above, this reasoning is flawed. However, even under the lesser standard for voluntarily produced information, the corporate names must still be disclosed. This is because the type of information at issue – the identities of corporations – is not "of a kind that would customarily not be released to the public by the person from whom it was obtained." *Critical Mass Energy Project*, 975 F.2d at 879.

DHS further muddles the argument for confidentiality by asserting that the information should be considered confidential because "DOD expressly promised that [company] participation would be confidential." DHS Motion at 29; *see also* Herrington Decl. at ¶¶ 7-8. A similar promise of confidentiality was made by the Internal Revenue Service in *Green v. Dept. of Commerce*, 489 F. Supp. 977 (D.D.C. 1980). There, the Court stated:

> [The Department of Commerce] claims that an unwarranted, albeit good faith, assurance of confidentiality may serve as the basis for a finding that the assurance must be honored, les the ability of the government to gather future information be impaired. To accepted defendant's contention, would create a gap in the FOIA

> large enough to eviscerate the Act. . . . Thus, the Court concluded that defendant's mere promise of confidentiality could not serve as the sole basis for withholding documents under [Exemption 4].

Id. at 980; *See also Tax Reform Research Group v. IRS*, 1974 WL 536 (D.D.C. 1974) ("it is well settled in this circuit 'that a District Court has no equitable jurisdiction to permit withholding of information which does not fall within one of the exemptions of the Act.'").[7] As in *Green*, here a promise of confidentiality by the government cannot prevent disclosure of non-private information under the FOIA.

To hold that the mere identity of a corporation could be withheld under Exemption 4 would create a black hole for all access requests concerning business records in the possession of a federal agency. Companies could routinely assert that even their identities should not be revealed to the requester. Such an outcome is far beyond the scope of the Exemption. Exemption 4 "is intended to encourage individuals to provide certain kinds of confidential information to the government, and it must be read narrowly in accordance with that purpose." *Nat'l Parks and Conservation Ass'n*, 498 F.2d at 768, *citing Soucie v. David*, 448 F.2d 1067 (D.C. Cir. 1971).

V. DHS Cannot Withhold Information Under Exemption 5 That Was Not "Inter-agency or Intra-agency Memorandums or Letters"

DHS improperly withholds a communication from AT&T to the agency under Exemption 5. Exemption 5 exempts from disclosure "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency." 5 U.S.C. § 552(b)(5) (2013). In order to withhold records under this exemption, the agency must demonstrate that the records it seeks to withhold are communications between agencies, or between staff of the same agency. *Fed. Open Mkt. Comm. of the Fed. Reserve Sys. v.*

[7] The Court in *Tax Reform Research Group* further emphasized that the FOIA was passed into law by Congress 3 years prior to the promise of confidentiality, and thus the promises were "rendered *ultra vires* three years before they were made." 1974 WL 536 at •3. Here, both defendants and the relevant corporations should have been well aware that the identification of the program participants could be compelled under the FOIA.

Merrill, 443 US 340, 352 (1979). In this case, DHS attempts to withhold a forwarded email from AT&T – one of the DIB program participants. *See* Exhibit 6. AT&T is not an "agency" subject to Exemption 5 protection, and its communication with the agency cannot be withheld under the deliberative process privilege.

Contrary to DHS's assertion, Exemption 5 applies to communications from private parties *only* when they are acting as agency consultants or advisors. *Dep't of Interior v. Klamath Water Users Protective Ass'n*, 532 U.S. 1, 11 (2001). In order to meet this standard, the consultant must meet a standard of objectivity. The Supreme Court explained, "…the consultant does not represent an interest of its own, or the interest of any other client, when it advises the agency that hires it. Its only obligations are to truth and its sense of what good judgment calls for, and in those respects the consultant functions just as an employee would be expected to do." *Id*. This Court has subsequently found that the agency is required to demonstrate the independent, consultative nature of the private party whose communications it wishes to withhold. *People for the American Way Foundatiob v. Dep't of Education,* 516 F. Supp. 2d 28, 39 (D.D.C. 2007). *See also Comptel v. Fed. Commc'ns Comm'n,* 910 F. Supp. 2d 100, (D.D.C. 2012). The court's application of *Klamath* in *Comptel* is instructive:

> The Court agrees that FCC has not met its burden to show that communications with SBC or USAC should be considered inter- or intra-agency in nature. The Court doubts, and the FCC has provided no evidence to the contrary, that communications with SBC could meet the requirements for consultant corollary outlined by *Klamath* and other relevant cases. . . . While communications with USAC are more likely qualify as inter-agency in nature, the FCC must explain why this would be the case.

Id. at 118-19

Here, DHS has not even attempted to argue that AT&T meets the standard for objectivity required by the "consultant corollary." In its *Vaughn* index, the agency merely refers to the request of AT&T, an Internet service provider ("ISP"). The Vaughn states, "DHS counsel

requested information from DHS program officials regarding a meeting to address inquiries about the DIB program from an ISP. DHS program officials discussed the proposed meeting and speculated about the reason for the ISP's meeting request." Dkt. 53-4 at 132. AT&T, a program participant, is not acting "just as an employee would be expected to do." *Klamath*, 532 U.S. at 11. The agency "speculated about the reason for the ISP's meeting request," indicating that the agency and AT&T were not acting in concert. AT&T was "advocating its own interests," rather than advising DHS on the agency's interests. *People For The Am. Way Found.*, 516 F. Supp. 2d at 39. Moreover, DHS makes no argument that AT&T should qualify as a consultant. Since the agency bears the burden of proof as to its use of exemptions, 5 U.S.C. § 552(a)(4)(B) ("the burden is on the agency to sustain its action"), the Court should hold for EPIC on the applicability of Exemption 5 to this document.

VI. DHS Cannot Withhold Information Under Exemption 7 That Was Not Furnished By A Confidential Source

DHS misconstrues the type of record that can be withheld under Exemption 7(D), and improperly withholds non-exempt records. Exemption 7(D) applies only to "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information could reasonably be expected to disclose the identity of a confidential source… which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source" 5 U.S.C. § 552(b)(7)(D) (2013).

Contrary to DHS' assertion, Exemption 7(D) is only appropriate when law enforcement agencies receive confidential information from an independent entity that seeks to withhold its

identity. The two categories of records protected under Exemption 7(D) are those which would disclose "the identity of a confidential source," if the information was furnished on a confidential basis, and "information furnished by a confidential source," if compiled by a law enforcement authority during the course of a criminal investigation. 5 U.S.C. § 552(b)(7)(D). *See also Adionser v. Dep't of Justice*, 811 F. Supp. 2d 284, 299 (D.D.C. 2011) *aff'd in part sub nom. Adionser v. U.S. Dep't of Justice*, 11-5093, 2012 WL 5897172 (D.C. Cir. Nov. 5, 2012). Both of these categories describe the "confidential source" as the entity that provides, or "furnishes," information to the government. Exemption 7(D) protects those "confidential sources" when their relationship to the government is that of an informant. *Id*.

Although many courts have offered interpretations of the word "confidential" for the purposes of Exemption 7(D) analysis, DHS' misapplication of the exemption in this case stems from the meaning of the term "source." Merriam Webster defines "source" as "one that supplies information." *Merriam-Webster.com*. Merriam-Webster, n.d. Web. 21 Sept. 2013.[8] In fact, the emphasis on the source as the supplier of information is evident from FOIA's conception. In the original text of the FOIA, Congress used the term "informer" to describe the type of information flow it sought to protect under Exemption 7(D). Freedom of Information Act and Amendments of 1974 (P.L. 93-502), Source Book: Legislative History, Texts and Other Documents at 133-34 and 192 (Joint Comm. Print 1975). It was only in the 1974 Amendments that the term "confidential source" was substituted for the word "informer" in the exemption. *Church of Scientology of California v. Dep't of Justice*, 612 F.2d 417, 422 (9th Cir. 1979). By broadening the wording of the statute, Congress clarified that many entities could qualify for protection under Exemption 7(D), rather than only individuals. *Id*.

[8] *Available at* http://www.merriam-webster.com/dictionary/source.

However, Exemption 7(D) protects these entities in their capacity as *sources*; that is, when they have a relationship with the federal law enforcement agency that is characterized by furnishing the government with information. In the first category of Exemption 7(D) protection, records may be exempt from the FOIA when their disclosure would reveal the identity of a source; in the second category, when the record contains information provided by a source. Both of these categories require the law enforcement agency to have entered into a relationship whereby the government is the recipient of information.

DHS has furnished no evidence that the information withheld under Exemption 7(D) was related specifically to instances when program participants were acting in a "source" capacity and not as the recipient of government-furnished information. DHS invokes Exemption 7(D) to withhold records documenting exchanges of information between DIB participants and the government. *See* Vaughn Index at 44-5, Document 90; Vaughn Index at 102-3, Document 209;Vaughn Index at 103, Document 210; Vaughn Index at 105-6, Document 214; Vaughn Index at 144-5, Document 306; Vaughn Index at 180-1, Document 404; Vaughn Index at 181-2, Document 405; Vaughn Index at 187, Document 419; Vaughn Index at 193, Document 433; Vaughn Index at 198-9, Document 444; Vaughn Index at 201-2, Document 449; Vaughn Index at 44-5, Document 90; Vaughn Index at 204, Document 454; Vaughn Index at 208-22, Withheld-in-Full Documents 8, 10-11, 13, 17-19, 24-25. In order to justify this withholding, the government states summarily in its Motion for Summary Judgment, "the DIB companies served as confidential sources of law enforcement information." DHS Motion at 40. The Motion cites to the declaration of Mark Herrington for the proposition that "[t]he program is voluntary, and… if the companies choose they can share cyber incident data back with DoD, including samples of malicious code that companies find in their networks." Herrington Decl. at ¶ 14. However, in the

next sentence, the government explains, "DoD uses that information to alert participating companies as well as the rest of the federal government to signatures of the captured malware." *Id*. Thus, the substance of the DIB program was the sharing of malware information to the program participants. While there was an option for participants to provide feedback to the government, even under a promise of confidentiality, that optional exchange of information was tangential to the primary activity of the program: the distribution of information from the government to individual participants. The main flow of information was not from DIB participants to the government, but from the government to the participants and DHS has provided no evidence that any other exchange of information was at issue in the documents containing the withheld information.

Even the broad definition of "source" under Exemption 7(D) cannot encompass the relationship between the DIB program participants and DHS. By DHS' own admission, the basic structure of the DIB program was that "DoD, in partnership with the Department of Homeland Security, shared classified threat information and the know-how to employ it with participating defense companies or their Internet providers to help them in defending their computer networks from attack or exploitation." Herrington Decl. at ¶ 13. The "source" of the information that DoD describes here were not the participating companies, but the law enforcement agency itself. The declarations that provide the basis for DHS' Motion for Summary Judgment describe a program in which the "informer," or "supplier of information," was the Agency seeking to withhold that information. *Id*.; *see also* DHS Motion at 2 ("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 relationship between participants and law enforcement agency was not contemplated by Congress in crafting

Exemption 7(D), and neither the text of the statute nor FOIA case law permits the federal government to protect itself as the a "confidential source" in an information-sharing program. *See Retail Credit Co. v. FTC,* No. 75-0895, 1976 WL 1206, at *4 n. 3 (D.D.C. 1976).

VII. DHS Has Not Met Its Burden of Proof for Arguments Not Properly Put Before this Court

DHS' Final Vaughn Index cites Exemptions 7(C) and 7(F) as additional grounds for withholding Document 419. Vaughn Index at 187. DHS has provided no information on why these exemptions may apply in its Motion or any of the attached exhibits. Accordingly, this Court should hold for EPIC on the applicability of these additional exemptions to this document. *See* 5 U.S.C. § 552(a)(4)(B) ("the burden is on the agency to sustain its action."); *see also EPIC v. Dept. of Homeland Security*, 384 F. Supp. 2d 100, 106 (D.D.C. 2005). In addition, though DHS cited Exemption 5 as a reason for withholdings for Documents 440, 442, and 444, the Agency has provided no detail on the applicability of the exemption. Vaughn Index at 197-99. Accordingly, this Court should further hold that DHS has failed to meet its burden of proof as to Exemption 5 in those documents. *See* 5 U.S.C. § 552(a)(4)(B) ("the burden is on the agency to sustain its action."); *see also EPIC v. Dept. of Homeland Security*, 384 F. Supp. 2d 100, 106 (D.D.C. 2005).

CONCLUSION

For the foregoing reasons, EPIC asks the Court to deny Defendant's Motion for Summary Judgment and grant EPIC's Cross-motion for Summary Judgment.

Respectfully submitted,

MARC ROTENGERG
EPIC Executive Director

/s/ Amie Stepanovich
AMIE STEPANOVICH
JULIA HORWITZ*
JERAMIE SCOTT**
Electronic Privacy Information Center
1718 Connecticut Ave., NW
Suite 200
Washington, D.C. 20009
(202) 483-1140
Counsel for Plaintiff

* Ms. Horwitz is admitted to practice in the State of Maryland. Her application to the District of Columbia is pending.
** Mr. Scott is admitted to practice in the State of New York.

CERTIFICATE OF SERVICE

I hereby certify that on the 27th day of September 2013, I served the foregoing PLAINTIFF'S OPPOSITION TO DEFENDANT'S MOTION FOR SUMMARY JUDGMENT, CROSS-MOTION FOR SUMMARY JUDGMENT, AND REQUEST FOR ORAL HEARING, including all exhibits and attachments, by electronic case filing upon:

LISA ZEIDNER MARCUS
TAMRA T. MOORE
Trial Attorneys
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave. NW
Washington, DC 20530
Tel. (202) 305-8546
Fax (202) 305-8517
lisa.marcus@usdoj.gov

/s/ Amie Stepanovich
Amie Stepanovich
Counsel for Plaintiff