

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

ELECTRONIC PRIVACY INFORMATION)
CENTER,)
))
Plaintiff,)
))
v.)
))
THE UNITED STATES DEPARTMENT OF)
HOMELAND SECURITY,)
))
Defendant.)

Civil Action No. 1:11-cv-02261-JDB

DEFENDANT’S MOTION FOR SUMMARY JUDGMENT

Defendant United States Department of Homeland Security hereby moves the Court to enter summary judgment in Defendant’s favor pursuant to Rule 56(b) of the Federal Rules of Civil Procedure. Attached in support of this Motion are: (1) a statement of material facts not in dispute; (2) a Memorandum of Points and Authorities; (3) the Declaration of James Holzer, including a Vaughn Index; and (4) the Declaration of Julie Ferrell, including a Vaughn Index.

Dated: July 31, 2012

Respectfully submitted,

STUART F. DELERY
Acting Assistant Attorney General
Civil Division

JOHN R. TYLER
Assistant Branch Director
Federal Programs Branch

/s/ Jean-Michel Voltaire
JEAN-MICHEL VOLTAIRE (NY Bar)
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, DC 20530
Tel.: 202-616-8211
Fax: 202-616-8460

Attorneys for Defendant

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

ELECTRONIC PRIVACY INFORMATION)
CENTER,)
))
Plaintiff,)
))
v.)
))
THE UNITED STATES DEPARTMENT OF)
HOMELAND SECURITY,)
))
Defendant.)

Civil Action No. 1:11-cv-02261-JDB

DEFENDANT’S STATEMENT OF MATERIAL FACTS NOT IN DISPUTE

Pursuant to Local Civil Rule 7(h) of the Rules of the United States District Court for the District of Columbia, Defendant United States Department of Homeland Security (DHS) hereby submits the following statement of material facts as to which Defendant contends there is no genuine issue in connection with its motion for summary judgment under Rule 56(b) of the Federal Rules of Civil Procedure.

1. In April, 2011, EPIC submitted a FOIA request to the Department of Homeland Security (“DHS”), seeking disclosure of documents related to the use of social-networking websites for investigative or data gathering purposes. Specifically, EPIC requested five categories of documents:

1. all contracts, proposals, and communications between the federal government and third parties, including, but not limited to, H.B. Gar Federal, Palantir Technologies, and/or Berico Technologies, and/or parent or subsidiary companies, that include provisions concerning the capability of social media monitoring technology to capture, store, aggregate, analyze, and/or match personally-identifiable information;
2. all contracts, proposals, and communications between DHS and any states, localities, tribes, territories, and foreign governments, and/or their agencies or subsidiaries, and/or any corporate entities, including but not limited to H.B. Gary Federal, Palantir Technologies, and/or Berico Technologies, regarding the implementation of any social media monitoring initiative;

3. all documents used by DHS for internal training of staff and personnel regarding social media monitoring, including any correspondence and communications between DHS, internal staff and personnel, and/or privacy officers, regarding the receipt, use, and/or implementation of training and evaluation of documents;
4. all documents detailing the technical specifications of social media monitoring software and analytic tools, including any security measures to protect records of collected information and analysis; and
5. all documents concerning data breaches of records generated by social media monitoring technology.

DHS Processing of EPIC's FOIA Request

2. By letter dated April 28, 2011, DHS Privacy Office acknowledged receipt of EPIC's FOIA request and denied EPIC's requests for expedited processing and for status of a representative of the news media. James Holzer Decl. ¶ 10. DHS Privacy Office then tasked five of component agencies to conduct a complete search. Id. ¶¶ 12-14. These component agencies were the Management Directorate (MGMT), the Office of Operations Coordination and Planning (OPS), Immigration and Customs Enforcement (ICE), United States Citizenship and Immigration Services (USCIS), Federal Emergency management Agency (FEMA), the United States Coast Guard (USCG).

3. Later, in January 2012, DHS also tasked the United States Secret Service (USSS) to conduct a complete search for records responsive to EPIC's FOIA request. Id. at ¶ 14.

4. Of all the components initially tasked to search, only DHS Privacy Office, USCIS, and OPS located responsive documents. Holzer Decl. ¶ 19.

5. On January 10, 2012, the DHS completed the review of 341 pages of responsive records. Id. ¶ 15. Of those pages, the DHS released 175 pages in full and 110 pages partially released. Id. The DHS informed EPIC that it was withholding 56 pages in their entirety under FOIA exemptions 3, 4, 5, 6, 7(C), and 7(E). ¶ 15.

6. On February 6, 2012, DHS produced its second interim response consisting of 39 pages, of which 24 pages were released in full and 15 pages were released with minor redactions pursuant to FOIA exemptions 6, 7(C), and 7(E). ¶ 17.

7. After the DHS forwarded EPIC's FOIA request to the OPS with instructions to search for responsive records and to forward the documents to the DHS Privacy Office for a consolidated response, the OPS FOIA Office reviewed the request and determined that two of its offices are most likely to contain responsive records. Id. ¶ 26.

8. The OPS provides decisions support and assists the Secretary in carrying out her responsibilities throughout the homeland security department. Id. at ¶ 21. The two OPS program offices most likely to have responsive records were the National Operation Center (NOC) and the Contracting Office. Id. at ¶ 26. The OPS personnel searched these offices, including the Media Monitoring Center systems and emails. Id. at ¶ 27. They also searched for contracts by using search terms, including "H.B. Gary Federal," "Palantir Technologies," and "Berico Technologies." Id.

9. As a result of its searches, the OPS located 161 pages of responsive documents and provided them to the DHS Privacy Office for processing. Id. DHS produced the non-exempt records on January 10 and February 6, 2012.

10. The USCIS also searched for and located some responsive records. The USCIS oversees the lawful immigration to the United States. See Holzer Decl. ¶ 29. After reviewing EPIC's request, the USCIS determined that seven of its program offices are most likely to maintain records. Id. at ¶ 31. These offices were the Office of Contracting (CNT); Fraud Detection and National Security (FDNS); Office of Information Technology (OIT); Field Operations Directorate (FOD); Office of Security and Integrity (OSI); Office of Human Capital and Technology (HCT); and Office of Communication (OCOMM). Id. USCIS personnel

searched these offices, including the FDNS Enterprise Collaboration Network (ECN), which is an electronic database, and the outlook e-mails and paper files. Id. at ¶ 32. They also searched for contracts, using the search terms “H.B. Gary Federal”, “Palantir Technologies”, “Berico Technologies,” and “social media.” Id. ¶ 33.

11. As a result of its searches, the USCIS located some responsive records and forwarded them to the DHS Privacy Office for processing. These records were processed and non-exempt documents were produced to Plaintiff as part of the first interim response.

12. ICE also received a copy of Plaintiff’s FOIA request, conducted a comprehensive search and found no responsive records. Holzer Decl. ¶¶ 36-46. ICE is the principal investigative arm of DHS and the second largest investigative agency in the federal government. Id. at ¶ 36. Its primary mission is to promote homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration. Id.

13. After reviewing Plaintiff’s FOIA request, the ICE FOIA Office determined that the ICE program offices most likely to maintain responsive records were the Office of Homeland Security Investigations (HIS), Office of Acquisitions (OAQ), and Privacy Office. Id. at ¶ 39. ICE personnel searched these offices. Id. at ¶¶ 40-46. They also conducted electronic searches, including searching the PRISM system that tracks and manages procurement operations and Federal Procurement Data System (a public database containing information on most Federal Government contracts). Id. at ¶¶ 42-46. The search terms used were “H.B. Gary Federal”, “Palantir Technologies”, and “Berico Technologies,” “social media,” “Facebook,” “LinkedIn,” “Twitter,” and “MySpace.” Id. at ¶¶ 43-44. These searches located some contracts, but they were determined to be non-responsive after a review. Id. at ¶ 44.

14. Furthermore, the MGMT searched for responsive records and found none. Id. at 47-54. MGMT is a major operational component of DHS and has several responsibilities. Id. at ¶¶ 47-48. Upon MGMT's review of Plaintiff's FOIA request, it determined that two of its program offices were most likely to maintain responsive records. Id. at ¶ 51. These offices were the Chief Information Officer (OCIO) and Office of Procurement Operations (OPO). Id.

15. MGMT staff conducted a search of the computer systems SOC On-Line and Security Incident Database, the PRISM computer system in which contracts information are stored, using search terms "social media monitoring" and "media monitoring." Id. at ¶¶ 52-53. No responsive records were located. Id.

16. Additionally, the USCG also conducted a comprehensive search and did not locate any responsive records. Id. at ¶¶ 55-66. The USCG is the only military organization within the Department of Homeland Security, and is responsible to safeguard the Nation's maritime interests and environment around the world. Id. at ¶ 55. Upon reviewing Plaintiff's FOIA request, the USCG FOIA Office determined that two of its program offices were most likely to maintain responsive records. Id. at ¶ 59. The offices were the Office of Public Affairs and Office of Intelligence. Id. USCG staff conducted a search of these offices' electronic databases and email files, but no responsive records were located. Id. at ¶¶ 60-61.

B. The United States Secret Service's Processing of Plaintiff's FOIA Request

17. On January 12, 2012, the Secret Service received a copy of Plaintiff's FOIA request from the DHS Privacy Office. Julie Ferrell Decl. ¶ 5. After reviewing the request, the Secret Service FOIA/PA Office determined that seven of its programs offices were most likely to have responsive records. Id. at ¶ 8. These offices were the Office of Investigations ("INV"); the Criminal Investigative Division ("CID"); the Procurement Division ("PRO"); the James J. Rowley Training Center ("JJRTC"); the Office of Chief Counsel ("LEG"); the Information

Resource Management Division (“IRMD”); and the Strategic Intelligence and Information Division (“SII”). Id. The staffs of these offices searched for records, including searching their respective databases and emails, using such search terms as Palantir Technologies”, “Berico Technologies”, “media monitor,” “social media,” “monitoring”, “internet”, and “Facebook.”

18. Given that the request asked for contracts and agreements, the Secret Service tasked PRO to search for responsive records. PRO is the contracting branch of the Secret Service and is responsible for the acquisition of all goods and services for the protective, investigative, and administrative missions of the Secret Service. Id. ¶¶ 13-15. Contracts entered into by the Secret Service are held in the division. Id. PRO conducted an electronic search of an internal database, called PRISM, to determine if any relevant contract actions existed. Id. PRISM contains, among other information, a record of all finalized contracts, as well as information on requests for certain proposals and requests for quotes that have been entered into the system. Id. PRO staff performed electronic queries using various terms including “Palantir Technologies”, “Berico Technologies”, and “media monitor”. Id. ¶ 14.

19. After reviewing the search results, PRO determined that one contract and one contract modification were potentially responsive to the request. Id.

20. Several Secret Service directorates located responsive records. After reviewing the potentially responsive records, the Secret Service determined that 365 pages of records received from LEG, CID, PID, SII, and the Protective Intelligence and Assessment Division (“PID”) were responsive to the Plaintiff’s request. Id. at ¶ 26. The Secret Service FOIA/PA Office processed these responsive records. Id.

21. On July 2, 2012, through the DOJ and on behalf of DHS, the Secret Service released fifty-five pages of records with no exemptions claimed to the Plaintiff. Id. at ¶27. After completing its review, on July 9, 2012, the Secret Service produced 32 additional pages of

records in full without redactions, 48 pages partially redacted pursuant to FOIA exemptions (b)(4), (b)(6), (b)(7)(C) and (b)(7)(E), and informed Plaintiff that 230 pages were withheld in their entirety pursuant to FOIA exemptions (b)(4), (b)(5), (b)(6), (b)(7)(C) and (b)(7)(E). Id. at ¶ 28.

22. The attached Declarations of James Holzer and Julie Ferrell provide a detailed explanation of the documents at issue and the justification for the withholdings.

Dated: July 31, 2012

Respectfully submitted,

STUART F. DELERY
Acting Assistant Attorney General
Civil Division

JOHN R. TYLER
Assistant Branch Director
Federal Programs Branch

/s/ Jean-Michel Voltaire
JEAN-MICHEL VOLTAIRE (NY Bar)
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, DC 20530
Tel.: 202-616-8211
Fax: 202-616-8460

Attorneys for Defendant

and/or Berico Technologies, regarding the implementation of any social media monitoring initiative;

3. all documents used by DHS for internal training of staff and personnel regarding social media monitoring, including any correspondence and communications between DHS, internal staff and personnel, and/or privacy officers, regarding the receipt, use, and/or implementation of training and evaluation of documents;
4. all documents detailing the technical specifications of social media monitoring software and analytic tools, including any security measures to protect records of collected information and analysis; and
5. all documents concerning data breaches of records generated by social media monitoring technology.

A. DHS Processing of EPIC's FOIA Request

By letter dated April 28, 2011, DHS Privacy Office acknowledged receipt of EPIC's FOIA request and denied EPIC's requests for expedited processing and for status of a representative of the news media. James Holzer Decl. ¶ 10. DHS Privacy Office then tasked five of component agencies to conduct a complete search. Id. ¶¶ 12-14. These component agencies were the Management Directorate (MGMT), the Office of Operations Coordination and Planning (OPS), Immigration and Customs Enforcement (ICE), United States Citizenship and Immigration Services (USCIS), Federal Emergency management Agency (FEMA), the United States Coast Guard (USCG). Later, in January 2012, DHS also tasked the United States Secret Service (USSS) to conduct a complete search for records responsive to EPIC's FOIA request. Id. at ¶ 14.

Of all the components initially tasked to search, only DHS Privacy Office, USCIS, and OPS located responsive documents. Holzer Decl. ¶ 19. On January 10, 2012, the DHS completed the review of 341 pages of responsive records. Id. ¶ 15. Of those pages, the DHS released 175 pages in full and 110 pages partially released. Id. The DHS informed EPIC that it was withholding 56 pages in their entirety under FOIA exemptions 3, 4, 5, 6, 7(C), and 7(E). ¶ 15. On February 6, 2012, DHS produced its second interim response consisting of 39 pages, of

which 24 pages were released in full and 15 pages were released with minor redactions pursuant to FOIA exemptions 6, 7(C), and 7(E). ¶ 17.

After the DHS forwarded EPIC's FOIA request to the OPS with instructions to search for responsive records and to forward the documents to the DHS Privacy Office for a consolidated response, the OPS FOIA Office reviewed the request and determined that two of its offices are most likely to contain responsive records. Id. ¶ 26. The OPS provides decisions support and assists the Secretary in carrying out her responsibilities throughout the homeland security department. Id. at ¶ 21. The two OPS program offices most likely to have responsive records were the National Operation Center (NOC) and the Contracting Office. Id. at ¶ 26. The OPS personnel searched these offices, including the Media Monitoring Center systems and emails. Id. at ¶ 27. They also searched for contracts by using search terms, including "H.B. Gary Federal," "Palantir Technologies," and "Berico Technologies." Id. As a result of its searches, the OPS located 161 pages of responsive documents and provided them to the DHS Privacy Office for processing. Id. DHS produced the non-exempt records on January 10 and February 6, 2012.

The USCIS also searched for and located some responsive records. The USCIS oversees the lawful immigration to the United States. See Holzer Decl. ¶ 29. After reviewing EPIC's request, the USCIS determined that seven of its program offices are most likely to maintain records. Id. at ¶ 31. These offices were the Office of Contracting (CNT); Fraud Detection and National Security (FDNS); Office of Information Technology (OIT); Field Operations Directorate (FOD); Office of Security and Integrity (OSI); Office of Human Capital and Technology (HCT); and Office of Communication (OCOMM). Id. USCIS personnel searched these offices, including the FDNS Enterprise Collaboration Network (ECN), which is an electronic database, and the outlook e-mails and paper files. Id. at ¶ 32. They also searched for contracts, using the search terms "H.B. Gary Federal", "Palantir Technologies", "Berico Technologies," and "social

media.” Id. ¶ 33. As a result of its searches, the USCIS located some responsive records and forwarded them to the DHS Privacy Office for processing. These records were processed and non-exempt documents were produced to Plaintiff as part of the first interim response.

ICE also received a copy of Plaintiff’s FOIA request, conducted a comprehensive search and found no responsive records. Holzer Decl. ¶¶ 36-46. ICE is the principal investigative arm of DHS and the second largest investigative agency in the federal government. Id. at ¶ 36. Its primary mission is to promote homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration. Id. After reviewing Plaintiff’s FOIA request, the ICE FOIA Office determined that the ICE program offices most likely to maintain responsive records were the Office of Homeland Security Investigations (HIS), Office of Acquisitions (OAQ), and Privacy Office. Id. at ¶ 39. ICE personnel searched these offices. Id. at ¶¶ 40-46. They also conducted electronic searches, including searching the PRISM system that tracks and manages procurement operations and Federal Procurement Data System (a public database containing information on most Federal Government contracts). Id. at ¶¶ 42-46. The search terms used were “H.B. Gary Federal”, “Palantir Technologies”, and “Berico Technologies,” “social media,” “Facebook,” “LinkedIn,” “Twitter,” and “MySpace.” Id. at ¶¶ 43-44. These searches located some contracts, but they were determined to be non-responsive after a review. Id. at ¶ 44.

Furthermore, the MGMT searched for responsive records and found none. Id. at 47-54. MGMT is a major operational component of DHS and has several responsibilities. Id. at ¶¶ 47-48. Upon MGMT’s review of Plaintiff’s FOIA request, it determined that two of its program offices were most likely to maintain responsive records. Id. at ¶ 51. These offices were the Chief Information Officer (OCIO) and Office of Procurement Operations (OPO). Id. MGMT staff conducted a search of the computer systems SOC On-Line and Security Incident Database, the

PRISM computer system in which contracts information are stored, using search terms “social media monitoring” and “media monitoring.” Id. at ¶¶ 52-53. No responsive records were located. Id.

Additionally, the USCG also conducted a comprehensive search and did not locate any responsive records. Id. at ¶¶ 55-66. The USCG is the only military organization within the Department of Homeland Security, and is responsible to safeguard the Nation's maritime interests and environment around the world. Id. at ¶ 55. Upon reviewing Plaintiff's FOIA request, the USCG FOIA Office determined that two of its program offices were most likely to maintain responsive records. Id. at ¶ 59. The offices were the Office of Public Affairs and Office of Intelligence. Id. USCG staff conducted a search of these offices' electronic databases and email files, but no responsive records were located. Id. at ¶¶ 60-61.

B. The United States Secret Service's Processing of Plaintiff's FOIA Request

On January 12, 2012, the Secret Service received a copy of Plaintiff's FOIA request from the DHS Privacy Office. Julie Ferrell Decl. ¶ 5. After reviewing the request, the Secret Service FOIA/PA Office determined that seven of its programs offices were most likely to have responsive records. Id. at ¶ 8. These offices were the Office of Investigations (“INV”); the Criminal Investigative Division (“CID”); the Procurement Division (“PRO”); the James J. Rowley Training Center (“JJRTC”); the Office of Chief Counsel (“LEG”); the Information Resource Management Division (“IRMD”); and the Strategic Intelligence and Information Division (“SII”). Id. The staffs of these offices searched for records, including searching their respective databases and emails, using such search terms as Palantir Technologies”, “Berico Technologies”, “media monitor,” “social media,” “monitoring”, “internet”, and “Facebook.”

Given that the request asked for contracts and agreements, the Secret Service tasked PRO to search for responsive records. PRO is the contracting branch of the Secret Service and is

responsible for the acquisition of all goods and services for the protective, investigative, and administrative missions of the Secret Service. Id. ¶¶ 13-15. Contracts entered into by the Secret Service are held in the division. Id. PRO conducted an electronic search of an internal database, called PRISM, to determine if any relevant contract actions existed. Id. PRISM contains, among other information, a record of all finalized contracts, as well as information on requests for certain proposals and requests for quotes that have been entered into the system. Id. PRO staff performed electronic queries using various terms including “Palantir Technologies”, “Berico Technologies”, and “media monitor”. Id. ¶ 14. After reviewing the search results, PRO determined that one contract and one contract modification were potentially responsive to the request. Id.

Several Secret Service directorates located responsive records. After reviewing the potentially responsive records, the Secret Service determined that 365 pages of records received from LEG, CID, PID, SII, and the Protective Intelligence and Assessment Division (“PID”) were responsive to the Plaintiff’s request. Id. at ¶ 26. The Secret Service FOIA/PA Office processed these responsive records. Id. On July 2, 2012, through the DOJ and on behalf of DHS, the Secret Service released fifty-five pages of records with no exemptions claimed to the Plaintiff. Id. at ¶27. After completing its review, on July 9, 2012, the Secret Service produced 32 additional pages of records in full without redactions, 48 pages partially redacted pursuant to FOIA exemptions (b)(4), (b)(6), (b)(7)(C) and (b)(7)(E), and informed Plaintiff that 230 pages were withheld in their entirety pursuant to FOIA exemptions (b)(4), (b)(5), (b)(6), (b)(7)(C) and (b)(7)(E). Id. at ¶ 28.

ARGUMENT

A. Statutory Background and Standard of Review

FOIA generally mandates disclosure, upon request, of government records held by an agency of the federal government, except to the extent that such records are protected from disclosure by one of nine statutory exemptions. The “fundamental principle” behind FOIA is “public access to Government documents.” John Doe Agency v. John Doe Corp., 493 U.S. 146, 151 (1989). “The basic purpose of FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed.” NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 (1978). At the same time, Congress recognized “that legitimate governmental and private interests could be harmed by release of certain types of information and provided nine specific exemptions under which disclosure could be refused.” FBI v. Abramson, 456 U.S. 615, 621 (1982); see also 5 U.S.C. § 552(b). While these exemptions are to be “narrowly construed,” Abramson, 456 U.S. at 630, courts must not fail to give the exemptions “meaningful reach and application.” John Doe Agency, 493 U.S. at 152. The FOIA thus “represents a balance struck by Congress between the public’s right to know and the government’s legitimate interest in keeping certain information confidential.” Ctr. for Nat’l Sec. Studies v. U.S. Dep’t of Justice, 331 F.3d 918, 925 (D.C. Cir. 2003).

Summary judgment is the procedure by which courts resolve nearly all FOIA actions. See Reliant Energy Power Generation, Inc. v. FERC, 520 F. Supp. 2d 194, 200 (D.D.C. 2007). As with non-FOIA cases, summary judgment is appropriate when there is no genuine issue as to any material fact and the moving party is entitled to judgment as a matter of law. See Fed. R. Civ. P. 56(c); Diamond v. Atwood, 43 F.3d 1538, 1540 (D.C. Cir. 1995). For a defendant agency to prevail on a motion for summary judgment in FOIA litigation, it must satisfy two elements. First,

it must “demonstrate that [it] conducted an adequate search which was reasonably calculated to uncover all relevant documents. . . . Second, materials that are withheld must fall within a FOIA statutory exemption.” Leadership Conference on Civil Rights v. Gonzales, 404 F. Supp. 2d 246, 252-53 (D.C. Cir. 2005) (citations omitted). A court reviews an agency’s response to a FOIA request *de novo*. See 5 U.S.C. § 552(a)(4)(B). As discussed below, Defendant has satisfied both elements in this case because its components conducted adequate searches and released all responsive materials, except those that fall within a statutory exemption.

B. Defendant Conducted a Reasonable and Adequate Search for Responsive Documents

The Defendant should prevail on summary judgment because it undertook a search that was “reasonably calculated to uncover all relevant documents.” Weisberg v. U.S. Dep’t of Justice, 705 F.2d 1344, 1351 (D.C. Cir. 1983). On summary judgment in a FOIA case, the agency must demonstrate that it has conducted an adequate search – that is, “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). “There is no requirement that an agency search every record system.” Id. “[T]he issue to be resolved is not whether there might exist any other documents possibly responsive to the request, but rather whether the *search* for those documents was *adequate*.” Weisberg v. U.S. Dep’t of Justice, 745 F.2d 1476, 1485 (D.C. Cir. 1984); see also Meeropol v. Meese, 790 F.2d 942, 952-53 (D.C. Cir. 1986) (“A search is not unreasonable simply because it fails to produce all relevant material.”); Perry v. Block, 684 F.2d 121, 128 (D.C. Cir.1982).

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 micromanage 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 “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) (quoting Ground Saucer Watch, Inc. v. CIA, 692 F.2d 770, 771 (D.C. Cir. 1981)). The statute does not require “meticulous documentation [of] the details of an epic search.” Perry, 684 F.2d at127. “[A]ffidavits that explain in reasonable detail the scope and method of the search conducted by the agency will suffice to demonstrate compliance with the obligations imposed by the FOIA.” Id.

As described in the attached James Holzer Declaration, the DHS’s search was reasonably calculated to uncover all documents responsive to EPIC’s request. Shortly after receiving EPIC’s FOIA request, the DHS Privacy Office initiated its search. See Holzer Decl. ¶¶ 12-14. First, the DHS Privacy Office identified six components within the agency that were likely to contain responsive records. Id. It forwarded EPIC’s request to these components with instructions to conduct a comprehensive search for records. Id. Second, each component identified the subcomponents reasonably likely to have responsive records and directed them to search their files. See Holzer Decl. ¶¶ 21-65. Third, the subcomponents then identified the individuals with subject-matter expertise to review EPIC’s request and to search for responsive records. Id. Fourth, the agency’s staffs conducted manual and electronic searches, using broad search terms deriving directly from EPIC’s FOIA request. Thus, the searches conducted were tailored to the particular request, and were targeted to those sections and individuals within the various components of DHS that would be expected to have responsive records. The steps that DHS took to identify responsive records, as documented in detail in the James Holzer Declaration, constituted an adequate search meeting the Defendant’s FOIA obligations

The search conducted by the Secret Service was also reasonably calculated to locate all records responsive to EPIC's FOIA request. As described in the Julie Ferrell Declaration, on January 12, 2012, the Secret Service FOIA Office received a copy of EPIC's FOIA request from the DHS Privacy Office. See Julie Ferrell Decl. ¶ 5. Upon review of EPIC's request, the Secret Service identified seven of its divisions that may potentially have responsive records. Id. at ¶ 8. These divisions then tasked their employees with subject-matter expertise to conduct manual and electronic searches, including searches of emails and databases, for responsive records. See Id. ¶¶ 9-25. The search terms used included "social media," "monitoring," "internet," "Facebook," "Palantir Technologies," "Berico Technologies," and "media monitoring." Id. at ¶¶ 14, 20. As demonstrated in the Julie Ferrell Declaration, the Secret Service performed searches at the locations most likely to house responsive documents by directing personnel to search for responsive material. The steps and methods the Secret Service used to locate the information sought by Plaintiff met its obligations under FOIA. Lawyers' Comm. for Civil Rights of San Francisco Bay Area v. U.S. Dep't of Treasury, 534 F. Supp. 2d 1126, 1131 (N.D. Cal. 2008) (noting that an agency demonstrates the adequacy of its search by "'describ[ing] what records were searched, by whom, and through what processes.'" (citation omitted).

In sum, the DHS and its components searched all sources they identified as reasonably likely to contain responsive documents. Therefore, DHS satisfied the search requirements of FOIA.

II. DHS AND THE SECRET SERVICE PROPERLY WITHHELD RECORDS UNDER APPLICABLE FOIA EXEMPTIONS

In order to obtain summary judgment, an agency bears the burden of justifying its decision to withhold records pursuant to FOIA's statutory exemptions. See 5 U.S.C. § 552(a)(4)(B). To satisfy that burden, the agency must provide declarations that identify the information at issue and the bases for the exemptions claimed. See Summers v. Dep't of Justice, 140 F.3d 1077, 1080

(D.C. Cir. 1998). Courts review *de novo* the agency's use of a FOIA exemption to withhold documents. Wolf v. CIA, 473 F.3d 370, 374 (D.C. Cir. 2007). But as this Court has noted:

[T]he Court may grant summary judgment based solely on information provided in an agency's affidavits or declarations if they are relatively detailed and when they describe "the documents and the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemption, and are not controverted by either contrary evidence in the record nor by evidence of agency bad faith."

Strunk v. U.S. Dep't of Interior, 752 F. Supp. 2d 39, 42-43 (D.D.C. 2010) (quoting Military Audit Project v. Casey, 656 F.2d 724, 738 (D.C.Cir.1981)). Again, agency declarations are accorded "a presumption of good faith, which cannot be rebutted by 'purely speculative claims about the existence and discoverability of other documents.'" SafeCard Servs., 926 F.2d at 1200 (quoting Ground Saucer Watch, 692 F.2d at 771); see also Strunk, 2010 WL 4780845, at *2. "Ultimately, an agency's justification for invoking a FOIA exemption is sufficient if it appears logical or plausible." Wolf, 473 F.3d at 374-75 (internal quotation marks and citations omitted).

As explained in detail below and in the attached Declarations, DHS and the Secret Service processed the responsive documents in accordance with FOIA and withheld certain information pursuant to FOIA Exemptions 4, 5, 6, 7(C), and 7(E). Each component properly invoked these exemptions, and processed and released all reasonably segregable information from the responsive records. Therefore, Defendant is entitled to summary judgment.

A. The USSS Properly Withheld Documents Pursuant to Exemption 4

FOIA exempts from disclosure "trade secrets and commercial or financial information obtained from a person and privileged or confidential." 5 U.S.C. § 552b(4) ("Exemption 4"). To withhold information under Exemption 4, the government agency must demonstrate that it is "(1) commercial and financial information, (2) obtained from a person or by the government, (3) that is privileged or confidential." GC Micro Corp. v. Def. Logistics Agency, 33 F.3d 1109, 1112 (9th Cir.1994). Commercial or financial matter is "confidential" for purposes of the exemption "if

disclosure of the information is likely to have either of the following effects: (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.

The Secret Service withheld information in documents 1, 2, 3, 4, 5, 6, 11, 14, 16, 17, 28, 29, 32, 33, and 35 on the basis of FOIA Exemption 4. (Ferrell Decl. ¶¶ 32-33; USSS Vaughn Index at pp. 1-4, 7-10, 15, 17-18.) A company prepared these documents as part of a contract bid submitted to the USSS. Id. They contain information regarding the pricing, technical specifications, and performance capabilities of the company. Id. It is information that is not customarily disclosed to the public by the company, and the company provided this information with the expectation that it would not be disclosed outside of the government. Id. Therefore, the Secret Service properly withheld this information because releasing it would impair the ability of the government to obtain necessary information from commercial suppliers in the future and impact the accuracy and full availability of such information.

B. DHS Properly Redacted Information Pursuant to Exemption 4

DHS redacted proprietary and confidential business information in several documents under Exemption 4. See DHS Vaughn Index pp. at 2-4. As demonstrated in the Vaughn Index attached to James Holzer Declaration, DHS redacted commercial information provided by a company in a contract bid submitted to OPS. Id. These documents contain the company's pricing information and its proposed evaluation plan. Id. This information is protected by trade secret and commercial or financial information obtained from a company that is privileged or confidential. Id. Disclosing this information would discourage other companies from providing confidential, accurate, and reliable business information to the government. Therefore, the DHS properly redacted this information to ensure that it obtains confidential business information in the future and to protect the submitters from competitors.

C. USSS Properly Withheld Documents Under Exemption 5 Attorney-Client Privilege

Exemption 5 exempts from mandatory disclosure “inter-agency or intra-agency memorandums or letters which would not be available by law to a party . . . in litigation with the agency.” 5 U.S.C. § 552(b)(5). In particular, it “exempt[s] those documents . . . [that are] normally privileged in the civil discovery context.” NLRB v. Sears, Roebuck & Co., 421 U.S. 132, 149 (1975). Exemption 5 incorporates the common law and executive privileges, including the deliberative process privilege, the attorney-client privilege, and the work product doctrine. In this case, the Secret Service has withheld materials in whole under Exemption 5 because they are protected under the attorney-client privilege.

The attorney-client privilege protects “confidential communications between an attorney and his client relating to a legal matter for which the client has sought professional advice.” Mead Data Cen., Inc. v. U.S. Dep’t of the Air Force, 566 F.2d 242, 252 (D.C. Cir. 1977). The attorney-client privilege is not limited to the context of litigation. Rein v. U.S. Patent & Trademark Office, 553 F. 3d 353, 377 (4th Cir. 2009) (noting that privilege “extends beyond communications in contemplation of particular litigation to communications regarding ‘an opinion on the law’”). The attorney-client privilege “protects a client’s confidences to her attorney so that the client may have uninhibited confidence in the inviolability of her relationship with her attorney.” Nat’l Res. Def. Council v. U.S. Dept. of Def., 388 F. Supp. 2d 1086, 1099 (C.D. Cal. 2005). To withhold a document under Exemption 5 pursuant to the attorney-client privilege, “an agency must demonstrate that the document it seeks to withhold (1) involves confidential communications between an attorney and his client and (2) relates to a legal matter for which the client has sought professional advice.” Id.

The Secret Service withheld documents 7, 8 and 9 on the basis of attorney-client privilege under FOIA Exemption 5. (Ferrell Decl. ¶ 35; USSS Vaughn Index at pp. 4-5). These documents, which are also being withheld under Exemption 7(E), are handwritten notes of attorneys within the Office of General Counsel (“OGC”) and an email communication between

Agency employees and Agency counsel. Id. They are about confidential facts supplied by the Secret Service Protective Intelligence and Assessment Division and its contractor working within the agency at various meetings with OGC counsel. Id. They contain information regarding data retention capabilities of a system utilized in identifying and analyzing threats against Secret Service protectees. Id. These notes also contain USSS attorneys' legal advice to the client agency based on those facts. Id. Because these documents reflect confidential communications between Agency counsel and their client relating to a legal matter for which the client sought professional advice, they are protected from disclosure under the attorney-client privilege. Releasing these documents would intrude upon the attorney-client relationship and discourage frank and open discussions between the Secret Service and agency counsel. See Schlefer v. United States, 702 F.2d 233, 244 n.26 (D.C. Cir. 1983).

D. DHS Properly Withheld Documents Under Exemption 5 Deliberative Process Privilege

The DHS properly withheld documents under Exemption 5 deliberative process privilege. Documents subject to the deliberative process privilege and therefore exempt from release include those “reflecting advisory opinions, recommendations and deliberations comprising part of a process by which governmental decisions and policies are formulated.” NLRB, 421 U.S. at 150. 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.

Dep't of Interior v. Klamath Water Users Protective Ass'n, 532 U.S. 1, 8-9 (2001) (internal quotation marks and citations omitted). “[E]fficiency of Government would be greatly hampered if, with respect to legal and policy matters, all Government agencies were prematurely forced to ‘operate in a fishbowl.’” EPA v. Mink, 410 U.S. 73, 87 (1973) (abrogated by statute on other grounds, Pub. L. No. 93-502, 88 Stat. 1561 (1974)).

“In deciding whether a document should be protected by the privilege [courts] look to whether the document is ‘predecisional’ [—] whether it was generated before the adoption of an agency policy

[—] and whether the document is ‘deliberative’ [—] whether it reflects the give-and-take of the consultative process.” Coastal States Gas Corp. v. Dep’t of Energy, 617 F.2d 854, 866 (D.C. Cir. 1980). “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) (citing Formaldehyde Inst. v. HHS, 889 F.2d 1118, 1223 (D.C. Cir. 1989)). In addition, “[t]here 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.’” Chemical 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 NLRB, 421 U.S. at 151).

In this case, the DHS identified three draft documents that are protected under the deliberative process privilege and withheld them on the basis of FOIA Exemption 5. See James Holzer Decl. ¶¶ 69-71; DHS Vaughn Index at pp.6-8, 17. The first document is a draft concept of operations that describes the characteristics of the proposed social medial monitoring and situational awareness from the viewpoints of the users of the system. Id. The second is a draft internal handbook discussing how the department will engage in social media monitoring and situational awareness. Id. The third document is a draft memorandum analyzing guidelines for use of Remote Retrievable Disposable Desktop. James Holzer Decl. ¶ 71; DHS Vaughn Index at p.17. These draft documents are protected under the deliberative process privilege because draft materials, and the drafting process itself are inherently predecisional and deliberative. See, e.g., Dudman Comms. Corp. v. Dep’t of Air Force, 815 F.2d 1565, 1569 (D.C. Cir. 1987) (disclosure of “decisions to insert or delete material or to change a draft’s focus or emphasis — would stifle the creative thinking and candid exchange of ideas necessary to produce good historical work”); Marzen v. HHS, 825 F.2d 1148, 1155 (7th Cir. 1987) (Exemption

5 “protects not only the opinions, comments and recommendations in the draft, but also the process itself”); In re Apollo Group, Inc. Sec. Litig., 251 F.R.D. 12, 31 (D.D.C. 2008) (“[D]raft documents by their very nature, are typically predecisional and deliberative, because they reflect only the tentative view of their authors; views that might be altered or rejected upon further deliberation either by their authors or by superiors.”) (non-FOIA case) (quotations omitted); Citizens for Resp. and Ethics in Washington v. DHS, 514 F. Supp. 2d 36, 46 (D.D.C. 2007) (applying privilege to draft “situation reports”); People for the Am. Way Found. v. Nat’l Park Serv., 503 F. Supp. 2d 284, 303 (D.D.C. 2007) (“drafts are commonly found exempt under the deliberative process exemption.”); Exxon Corp. v. Dep’t of Energy, 585 F. Supp. 690, 697-98 (D.D.C. 1983) (“[d]raft documents by their very nature, are typically predecisional and deliberative”). Disclosure of draft materials would expose individual employees’ contributions to the drafting process to public scrutiny, which would likely inhibit deliberations, and, ultimately, inhibit the frank and candid exchange of information and expression of ideas, both within DHS and its component agencies. see, e.g., Russell v. Dep’t of Air Force, 682 F.2d 1045, 1048 (D.C. Cir. 1982) (recognizing that disclosure of draft manuscript could stifle candor in the drafting process and lead to confusion of the public). Therefore, the DHS properly withheld these draft documents under Exemption 5 deliberative process privilege.

E. The USSS Properly Withheld and Redacted Documents Pursuant to Exemptions 6 and 7(C)

The Secret Service properly invoked Exemption 6 and Exemption 7C to withhold names and identifying information of its (1) law enforcement personnel and (2) third parties mentioned in law enforcement records.

Exemptions 6 and 7(C) protect the privacy of individuals from unwarranted invasion. The applicability of both of these exemptions requires the agency to balance the relevant individual privacy rights against the public interest in disclosure. Exemption 6 allows the withholding of information about individuals in “personnel and medical files and similar files” when the disclosure of such information would constitute a “clearly unwarranted invasion of personal

privacy.” 5 U.S.C. § 552(b)(6). For this exemption to apply, the information at issue must be maintained in a government file and “appl[y] to a particular individual.” United States Dep’t of State v. Wash. Post Co., 456 U.S. 595, 602 (1982). Once this threshold requirement is met, Exemption 6 requires the agency to balance the individual’s right to privacy against the public’s interest in disclosure. See Reed v. NLRB, 927 F.2d 1249, 1251-52 (D.C. Cir. 1991).

Exemption 7(C) is similar, permitting the withholding of “records or information compiled for law enforcement purposes” to the extent that disclosure of such information “could reasonably be expected to constitute an unwarranted invasion of personal privacy.” 5 U.S.C. § 552(b)(7). Thus, where, as here, information or records at issue were compiled for law enforcement purposes, the balancing test tilts further in favor of non-disclosure. Exemption 7(C) has been applied in this case, together with Exemption 6, to protect personal identifying information, because the records at issue were all compiled for a law enforcement purpose. The information at issue here was compiled in connection with the Secret Service’s and certain DHS component’s protective mission and under their authority to conduct law enforcement activities, and thus was compiled for a law enforcement purpose. See Ferrell Decl. ¶ 38. The Secret Service and other DHS components, as law enforcement entities, are entitled to deference in this assessment. See Campbell v. Dep’t of Justice, 164 F.3d 20, 32 (D.C. Cir. 1998).

Courts have adopted a broad construction of the privacy interests protected by these two exemptions, rejecting a “cramped notion of personal privacy” and emphasizing that “privacy encompass[es] the individual’s control of information concerning his or her person.” Dep’t of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989) (construing Exemption 7(E)). Privacy is of particular importance in the FOIA context because a disclosure required by FOIA is a disclosure to the public at large. See, e.g., Painting & Drywall Work Pres. Fund, Inc. v. HUD, 936 F.2d 1300, 1302 (D.C. Cir. 1991). In contrast, “the only relevant public

interest in the [Exemption 6] balancing analysis [is] the extent to which disclosure of the information sought would shed light on an agency's performance of its statutory duties' or otherwise let citizens know what their government is up to." Dep't of Defense v. Fed. Labor Relation Auth., 510 U.S. 487, 497 (1994) (internal quotation marks omitted).

The Secret Service has redacted or withheld the names of law enforcement personnel and other personally identifying information in documents 6, 9, 11, 12, 13, and 15 to 42. See Ferrell Decl. ¶ 39. It also withheld the names, personal contact information and other identifying information of third parties who appear on the documents 1, 2, 3, 5, 6, 9 to 15, and 17 to 42. The Secret Service is withholding portions of these documents after concluding that disclosure would cause a clearly unwarranted invasion of personal privacy, which would not be counterbalanced by any public interest in the information. Id. Document 23 has been withheld in full because this twenty-four page-document consists of access forms that have been filled in by various individuals and contain such personally identifiable information as names, social security numbers, and dates of birth. Id. at ¶ 43. If this personally identifiable information was redacted from the document, all that would remain would be empty standard forms. Id. Therefore, the Secret Service is withholding this document in full pursuant to exemptions (b)(6) and (b)(7)(C).

The Secret Service has properly applied Exemption 6 and 7(C) to law enforcement records that identify law enforcement personnel and third parties. "The names of and identifying information about law enforcement officers are routinely withheld under Exemption 7(C) on the ground that such disclosure could reasonably be expected to constitute an unwarranted invasion of the officers' personal privacy." Concepcion v. FBI, 699 F. Supp. 2d 106, 112 (D.D.C. 2010). Privacy considerations support protecting the law enforcement personnel and private individuals, from unnecessary, unofficial questioning as to the conduct of this or other investigations, which could "subject them to annoyance or harassment in either their official or private lives."

Lewis-Bey v. Dep't of Justice, 595 F. Supp. 2d 120, 134-35 (D.D.C. 2009) (quoting Lesar v. Dep't of Justice, 636 F.2d 472, 487 (D.C. Cir. 1980)). When weighed against the lack of public interest in the identities of these individuals, this privacy interest justifies withholding.

F. DHS Properly Withheld and Redacted Documents Pursuant to Exemptions 6 and 7(C)

Applying the legal principles mentioned above, the DHS properly invoked exemptions 6 and 7(C) to redact the names of its law enforcement personnel, email tracking information, and other personal contact information of these employees and third parties to protect their privacy interests. See John Holzer Decl. ¶¶ 72-76; DHS Vaughn Index at pp. 2-5, 7-12, 13-18.

Releasing this personally identifiable information would constitute a clearly unwarranted invasion of the individuals' privacy. Id. Furthermore, the redacted information was compiled for law enforcement purpose, because the records were created by DHS law enforcement agencies during the course of a law enforcement activity. Id. Because of the strong privacy interest in law enforcement records, releasing the personal identifiable information could reasonably constitute an unwarranted invasion of personal privacy, as such disclosure might subject the third parties to negative harassment, criticism and suspicion. The personal privacy interest is stronger when disclosing the information would not serve the "core purpose" of the FOIA, i.e., to "shed light on an agency's performance of its statutory duties." DOJ v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 773 (1989). Therefore, the names and contact information were properly redacted pursuant to FOIA Exemptions 6 and 7(C).

G. The USSS Properly Withheld Documents Under FOIA Exemption 7(E)

FOIA protects from mandatory disclosure "records or information compiled for law enforcement purposes" when that 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). Congress intended that Exemption 7(E) protect from disclosure techniques and procedures used to prevent and protect against crimes, as well as techniques and procedures used to investigate crimes after they have been committed. See, e.g., PHE, Inc. v. Dep’t of Justice, 983 F.2d 248, 250–51 (D.C. Cir. 1993) (holding that portions of FBI manual describing patterns of violations, investigative techniques, and sources of information available to investigators were protected by Exemption 7(E)). This exemption applies even when the identity of the techniques has been disclosed, but the manner and circumstances of the techniques are not generally known, or the disclosure of the details could reduce their effectiveness. See Blanton v. U.S. Dep’t of Justice, 63 F. Supp. 2d 35, 49–50 (D.D.C. 1999); Coleman v. FBI, 13 F. Supp. 2d 75, 83 (D.D.C. 1998).

Exemption 7(E) is comprised of two clauses: the first relating to law enforcement “techniques or procedures,” and the second relating to “guidelines for law enforcement investigations or prosecutions.” 5 U.S.C. § 552(b)(7). The latter category of information may be withheld only if “disclosure could reasonably be expected to risk circumvention of the law.” Id. No such showing of harm is required for the withholding of law enforcement “techniques or procedures,” however, which receive categorical protection from disclosure. See Keys v. DHS, 510 F. Supp. 2d 121, 129 (D.D.C. 2007) (stating that first clause of Exemption 7 (E) “requires no demonstration of harm or balancing of interests”); Smith v. Bureau of Alcohol, Tobacco & Firearms, 977 F. Supp. 496, 501 (D.D.C. 1997); but see PHE, Inc. v. DOJ, 983 F.2d 248, 250 (D.C.Cir. 1993) (stating that under Exemption 7 (E), agency “must establish that releasing the withheld material would risk circumvention of the law.”); Piper v. DOJ, 294 F. Supp.2d 16, 30 (D.D.C. 2003).

As a threshold issue, the court must make a determination as to whether the documents have a law enforcement purpose, which, in turn, requires examination of whether the agency serves a

“law enforcement function.” Church of Scientology Intern. v. I.R.S., 995 F.2d 916, 919 (9th Cir. 1993) (internal quotation marks and citation omitted). However, a government agency with a clear law enforcement mandate ““need only establish a rational nexus between enforcement of a federal law and the document for which [a law enforcement] exemption is claimed.”” Rosenfeld v. U.S. Dept. of Justice, 57 F.3d 803, 808 (9th Cir. 1995) (citation omitted). Under the “rational nexus test,” courts “accord a degree of deference to a law enforcement agency’s decisions to investigate” and will not second-guess the agency’s investigative efforts “if there is a plausible basis for the decision.”” Id. (quoting Pratt v. Webster, 673 F.2d 408, 421 (D.C. Cir.1982)).

In this case, there is no doubt that the Secret Service and DHS have clear law enforcement mandates. See Nat’l Day Laborer Org. Network v. U.S. Immigration and Customs Enforcement Agency, 811 F. Supp. 2d 713, 744 (S.D.N.Y. 2011) (stating that ICE and DHS are “unquestionably federal law enforcement agencies”); U.S. News & World Report v. Dep’t of the Treasury, No. 84–2303, 1986 U.S. Dist. LEXIS 27634, at *5 (D.D.C. Mar. 26, 1986) (stating that while “[t]he Secret Service is unique in that its law enforcement efforts are geared primarily towards prevention rather than apprehension,” there “can be no doubt that they are directly related to the agency’s statutory mandate”). As law enforcement agencies, the Secret Service’s and DHS’s decisions to invoke exemption 7 (E) are entitled to deference. Campbell v. DOJ, 164 F.3d 20, 32 (D.C. Cir. 1998).

The Secret Service withheld portions of documents 12, 13, 15, 18, 21-23, 26-28, 30, 32-35, 37 and 48 that are responsive to Plaintiff’s request, and withheld in full documents 1-11, 14, 16, 17, 19 and 20 on the basis of Exemption 7(E). See Ferrell Decl. ¶ 44. The withholdings relate to information on a technique utilized by USSS in identifying, analyzing, and investigating potential threats against the President, Vice-President, and other Secret Service protectees, the specific guidelines used to identify potential threats, and information regarding systems and technology

used as part of that technique, including the name of the system and information on system vulnerabilities. Id. The release of this information would reveal techniques and methodologies used by the Secret Service that are not generally known to the public, and could nullify the future effectiveness of protective and investigative measures designed to identify and investigate threats, rendering them operationally useless. Id. at ¶ 45. Disclosure of this type of information, therefore, could impede the Secret Service's efforts to protect the President, Vice-President, and other protectees in the future. Id. For these reasons, the Secret Service is withholding in full 205 pages of material pursuant to exemption (b)(7)(E).

H. DHS Properly Withheld Information Under FOIA Exemption 7(E)

Having met the threshold of a law enforcement agency, DHS properly invoked Exemption 7 (E) to redact passwords, codes, and other information that would allow access to its databases and law enforcement computer systems, which contain law enforcement information about investigations or prosecutions. Holzer Decl. ¶¶ 77-78; DHS Vaughn Index at pp. 6, 7, 9, 11, 12, 14, 15, and 23. These access codes information are not known to the public and are used by law enforcement personnel to access the agency's electronic databases that have information on individuals subject to criminal investigations or prosecutions. Having concluded that the release of this information would allow unauthorized access to critical law enforcement information, which could result in tampering or other manipulation of information and thus inhibit investigative efforts, this information should be given categorical protection as information related to law enforcement techniques or procedures and are protected from disclosure under Exemption 7(E). See Keys v. DHS, 510 F. Supp. 2d at 129 (the agency needs to show only that the information would reveal a law enforcement technique that is unknown to the public)

Although it is unnecessary for DHS to demonstrate that the release of the law enforcement systems access information could reasonably be expected to risk the circumvention of the law, id.

that standard is satisfied in any event. Exemption 7(E) “exempts from disclosure information that *could increase the risks* that a law will be violated or that past violators will escape legal consequences.” Mayer Brown LLP v. IRS, 562 F.3d 1190, 1193 (D.C. Cir. 2009). Moreover, “[t]he exemption looks not just for circumvention of the law, but for a risk of circumvention; not just for an actual or certain risk of circumvention, but for an expected risk; not just for an undeniably or universally expected risk, but for a reasonably expected risk; and not just for certitude of a reasonably expected risk, but for the chance of a reasonably expected risk.” Id. This “relatively low bar . . . ‘only requires that the [agency] demonstrate logically how the release of the requested information might create a risk of circumvention of the law.’” Blackwell v. FBI, 646 F.3d 37, 42 (D.C. Cir. 2011) (quoting Mayer Brown, 562 F.3d at 1194). Because it is possible that criminals could use this information, if disclosed, to gain access to the agency’s law enforcement files and thereby evade detention, or that violators could use it to tamper with the source of information and thus inhibit investigative efforts, DHS properly withheld that information under Exemption 7(E). See PHE, Inc., 983 F.2d at 251.

Dated: July 31, 2012

Respectfully submitted,

STUART F. DELERY
Acting Assistant Attorney General
Civil Division

JOHN R. TYLER
Assistant Branch Director
Federal Programs Branch

/s/ Jean-Michel Voltaire
JEAN-MICHEL VOLTAIRE (NY Bar)
Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW
Washington, DC 20530
Tel.: 202-616-8211
Fax: 202-616-8460

Attorneys for Defendant

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

ELECTRONIC PRIVACY INFORMATION)	
CENTER,)	
)	
Plaintiff,)	
)	
v.)	Civil Action No. 1:11-cv-02261-JDB
)	
)	
THE UNITED STATES DEPARTMENT OF)	
HOMELAND SECURITY,)	
)	
Defendant.)	
_____)	

DECLARATION OF JAMES HOLZER

I, James V.M.L. Holzer, I, declare and state as follows:

1. I am the Director of Disclosure and FOIA Operations for the Department of Homeland Security (DHS) Privacy Office. In this capacity, I am the Department official immediately responsible for responding to requests for records under the Freedom of Information Act (FOIA), 5 U.S.C. § 552 (the FOIA), the Privacy Act, 5 U.S.C. § 552a (the Privacy Act), and other applicable records access provisions. I have been employed by the DHS Privacy Office (DHS Privacy) in this capacity since May 2011. I make the following statements based upon my personal knowledge, which in turn is based on a personal review of the records in the case files established for processing the subject request and upon information furnished to me in the course of my official duties.

2. Through the exercise of my official duties, I have become familiar with the background of this case and have read a copy of the complaint filed by plaintiff.

DHS FOIA Background and Organization

3. DHS Privacy is the Department of Homeland Security's Privacy Office. DHS Privacy partners with privacy staff in every DHS component to assess all new or proposed programs, systems, technologies or rule-makings for privacy risks, and recommend privacy protections and alternative methods for handling personal information to mitigate privacy risks. DHS Privacy also centralizes FOIA and Privacy Act operations to provide policy and programmatic oversight, and support implementation across the Department.

4. The Mission of DHS Privacy is to preserve and enhance privacy protections for all individuals, to promote transparency of Department operations, and to serve as a leader in the privacy community. DHS Privacy (1) evaluates Department legislative and regulatory proposals involving collection, use, and disclosure of personally identifiable information (PII); (2) centralizes FOIA and Privacy Act operations to provide policy and programmatic oversight, and support implementation across the Department; (3) operates a Department-wide Privacy Incident Response Program to ensure that incidents involving PII are properly reported, investigated and mitigated, as appropriate; (4) responds to complaints of privacy violations and provides redress, as appropriate; and (5) provides training, education and outreach to build a culture of privacy across the Department and transparency to the public.

5. Some of the DHS Components (example: United States Secret Service (USSS)) maintain a combined office that handles matters related to both the Privacy Act and the FOIA. Other Components (example: United States Immigration and Customs Enforcement (ICE))

maintain two separate offices, one for matters related to the Privacy Act and one for matters related to the FOIA.

6. Each Component maintains its own automated case tracking system which assigns case control numbers to, and tracks the status of, all FOIA and Privacy Act requests received by that Component. Components log all incoming FOIA and Privacy Act requests into their automated case tracking system, and input information about each request into the system (including, but not limited to, the requester's name and/or organization and, in the case of FOIA requests, the request's topic). All requesters are then notified of the case control numbers assigned to their requests. It is the custom of all Components to refer to the case control numbers in all correspondence with requesters. The automated case tracking systems are text searchable on a field-by-field basis.

DHS Privacy Processing of the FOIA Request

7. On April 19, 2011, DHS Privacy received a FOIA request from Plaintiff dated April 12, 2011.

8. DHS Privacy assigned the File No DHS/OS/PRIV/11-0736 to the request.

9. In the request, EPIC sought agency records in the possession of the Department of Homeland Security ("DHS") concerning private sector contracts, internal government trainings, inter-governmental communications and agreements, technical specifications, and security measures related to the agency's social media monitoring initiatives.

10. On April 28, 2011, DHS Privacy issued an acknowledgement to EPIC which denied EPIC's request for expedited processing of the FOIA request and EPIC's request for status as a representative of the news media.

11. DHS Privacy referred the FOIA request to other components as described below.

12. On April 26, 2011, DHS Privacy issued a memo tasking the Management Directorate (MGMT) and the Office of Operations Coordination and Planning (OPS)

13. On April 29, 2011, DHS Privacy issued a memo tasking Immigration and Customs Enforcement (ICE), United States Citizenship and Immigration Services (USCIS), Federal Emergency Management Agency (FEMA) and the United States Coast Guard (USCG) to conduct a search for responsive records within their offices.

14. On January 10, 2012, DHS Privacy issued a memo tasking the United States Secret Service (USSS) with searching for responsive documents.

15. On January 10, 2012, DHS Privacy issued its first interim response to EPIC. DHS Privacy indicated that it had completed its review of 341 pages. Of those pages, DHS Privacy determined that 175 pages of the records were releasable in their entirety, 110 pages were partially releasable, and 56 pages were withheld in their entirety pursuant to Title 5 U.S.C. § 552 (b)(3), (b)(4), (b)(5), (b)(6), (b)(7)(C), and (b)(7)(E), FOIA Exemptions 3,4,5,6, 7(C), and 7(E).

16. DHS Privacy provided appeal rights to the Plaintiff.

17. On February 6, 2012, DHS Privacy completed its second interim response which consisted of an additional 39 pages. Of those pages, DHS Privacy determined that 24 pages of the records were releasable in their entirety, and 15 pages are partially releasable pursuant to Title 5 U.S.C. § 552 (b)(6), (b)(7)(C), and (b)(7)(E), FOIA Exemptions 6, 7(C) and 7(E). DHS Privacy transmitted this response directly to the Department of Justice (DOJ) for handling in light of the current litigation. As far as DHS Privacy is aware, the second interim response was provided to EPIC by DOJ on February 15, 2012.

18. DHS Privacy provided appeal rights to the Plaintiff.

19. Of the components tasked to search, only PRIV, USCIS and OPS had responsive documents.

20. As of this date, DHS Privacy has not received any appeal regarding the adverse determination.

OPS Processing of FOIA Request

21. The Office of Operations Coordination (OPS) provides decision support and enables the Secretary's execution of responsibilities across the homeland security enterprise by promoting situational awareness and information sharing, integrating and synchronizing strategic operations and planning, and administering the DHS continuity program.

22. Pursuant to the *Homeland Security Act of 2002*, the Homeland Security Operations Center (HSOC) was established “to provide situational awareness and a common operating picture for the entire Federal Government, and for State, local, and tribal governments as appropriate, in the event of a natural disaster, act of terrorism, or other man-made disaster.” In 2005, as a result of the Second Stage Review, DHS created the Office of Operations Coordination as one of the new organizational initiatives to reshape the Department. The following year, the HSOC transitioned into the National Operations Center (NOC), which now serves as the primary National-level hub for domestic situational awareness by fusing law enforcement, intelligence, emergency response, private sector, and open-source reporting.

23. OPS is comprised of the Continuity Division, Operations Coordination Division, National Operations Center (NOC), Plans Division and Resources Division.

24. In a memorandum dated April 26, 2011, DHS Privacy forwarded a copy of Plaintiff's April 12, 2011 FOIA request to the OPS FOIA Office. DHS instructed the OPS FOIA Office to conduct a search for responsive records, to review any such records in accordance with the FOIA

for the purpose of release recommendations, and to provide any such recommendations to DHS Privacy for use in a consolidated response.

25. OPS assigned FOIA case number 12-OPS-009 to the Plaintiff's FOIA request.

26. The OPS FOIA Office determined that the OPS program offices most likely to maintain records that would be responsive to the Plaintiff's FOIA request were the NOC and the Contracting Office.

27. Within those offices, OPS personnel searched the Contracting Office and the Media Monitoring Center systems, including email. OPS personnel conducted a search for contracts that would be responsive to the FOIA request guided by search terms including "H.B. Gary Federal", "Palantir Technologies", and "Berico Technologies". OPS personnel identified 100 pages of responsive documents from the Contracting Office, the bulk of that being a Contract with General Dynamics. Another 61 pages were located in the Media Monitoring Center, most of which were training materials including a 39-page document entitled "Media Monitoring Capability Desktop Reference Binder."

28. These documents were turned over to the DHS Privacy office for processing and disclosure to the Requestor.

USCIS Processing of the FOIA Request

29. U.S. Citizenship and Immigration Services (USCIS) is the arm of DHS that oversees lawful immigration to the United States. USCIS provides accurate and useful information to customers, granting immigration and citizenship benefits, promoting an awareness and understanding of citizenship, and ensuring the integrity of the immigration system.

30. In a memorandum dated April 29, 2011, DHS Privacy forwarded a copy of Plaintiff's

April 12, 2011 FOIA request to the USCIS FOIA Office. DHS instructed the USCIS FOIA Office to conduct a search for responsive records, to review any such records in accordance with the FOIA for the purpose of release recommendations, and to provide any such recommendations to DHS Privacy for use in a consolidated response.

31. The USCIS FOIA Office determined that the USCIS program offices most likely to maintain records that would be responsive to the Plaintiff's FOIA request were the Office of Contracting (CNT); Fraud Detection and National Security (FDNS); Office of Information Technology (OIT); Field Operations Directorate (FOD); Office of Security and Integrity (OSI); Office of Human Capital and Technology (HCT); and Office of Communication (OCOMM).

32. Within those offices, USCIS personnel searched the FDNS Enterprise Collaboration Network (ECN), Outlook e-mails, and paper files in desk drawers.

33. USCIS personnel conducted a search for contracts that would be responsive to the FOIA request guided by search terms including "H.B. Gary Federal", "Palantir Technologies", "Berico Technologies," and "social media."

34. Of those offices, the following identified responsive documents: Fraud Detection and National Security (FDNS); Office of Information Technology (OIT); Field Operations Directorate (FOD); and Office of Security and Integrity (OSI).

35. These documents were turned over to the DHS Privacy office for processing and disclosure to the Requestor.

ICE Processing of the FOIA Request

36. U.S. Immigration and Customs Enforcement ("ICE") is the principal investigative arm of the U.S. Department of Homeland Security ("DHS") and the second largest investigative agency in the federal government. Created in 2003 through a merger of the investigative and

interior enforcement elements of the U.S. Customs Service and the Immigration and Naturalization Service, ICE now has more than 20,000 employees in offices in all 50 states and 47 foreign countries. ICE's primary mission is to promote homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration.

37. In a memorandum dated April 29, 2011, the DHS Privacy forwarded a copy of Plaintiff's April 12, 2011 FOIA request to the ICE FOIA Office. DHS instructed the ICE FOIA Office to conduct a search for responsive records within ICE, to review any such records in accordance with the FOIA for the purpose of release recommendations, and to provide any such recommendations to the DHS FOIA Office for use in a consolidated response.

38. ICE assigned FOIA case number 2011FOIA8456 to the Plaintiff's FOIA request.

39. Upon ICE's review of Plaintiff's FOIA request, the ICE FOIA Office determined that the ICE program offices most likely to maintain records that would be responsive to the Plaintiff's FOIA request were the ICE Office of Homeland Security Investigations, the ICE Office of Acquisitions, and the ICE Privacy Office. The ICE FOIA Office forwarded a copy of the Plaintiff's FOIA request to those programs and instructed those programs to conduct a comprehensive search for records and information that would be responsive to Plaintiff's FOIA request.

40. Within ICE HSI, the Section Chief of the ICE HSI Records and Disclosure Unit reviewed Plaintiff's FOIA request and determined that the ICE HSI Cyber Crimes Center and the Intellectual Property Rights Center ("IPR Center") were the two HSI programs most likely to maintain records that would be responsive to the Plaintiff's FOIA request.

41. The Section Chief of the ICE HSI Record and Disclosure Unit forwarded Plaintiff's

FOIA request to Special Agents within the HSI Cyber Crimes Center and the HSI IPR Center. After a careful review of the Plaintiff's FOIA request, those Special Agents in the HSI Cyber Crimes Center and the IPR Center informed the ICE FOIA Office that ICE HSI does not maintain any records that would be responsive to the Plaintiff's FOIA request. Further, those Special Agents informed the ICE FOIA Office that ICE HSI does not have a social media monitoring initiative as described in Plaintiff's FOIA request.

42. The ICE Office of Acquisitions ("ICE OAQ") is responsible for managing ICE's procurement operations. ICE OAQ facilitates the acquisition of goods and services through contracts. ICE OAQ uses the PRISM system to track and manage its procurement operations. PRISM provides comprehensive, Federal Acquisition Regulation based acquisition support, and contains information on all ICE and DHS procurement requisitions, solicitations, contracts, simplified acquisitions, interagency agreements, blanket purchase agreements, and basic ordering agreements.

43. ICE OAQ conducted a search of PRISM for contracts that would be responsive to the FOIA request guided by search terms including "H.B. Gary Federal", "Palantir Technologies", and "Berico Technologies". The search identified two ICE contracts with Palantir Technologies identified as HSCETE11F00125 and HSCEMD11P00040 but these documents were reviewed and deemed non-responsive. ICE OAQ informed the ICE FOIA Office that these two contracts (HSCETE11F00125 and HSCEMD11P00040) are for information technology support of the ICE Office of Homeland Security Investigation.

44. Further, a search of the Federal Procurement Data System ("FPDS") was conducted.

FPDS¹ is a publicly available database that contains information on all Federal contracts whose estimated value is \$3,000 or more or that may be \$3,000 or more. A search of FPDS using the term “H.B. Gary Federal” located zero contracts wherein ICE is assigned as the contracting agency. A search of FPDS using the term “Palantir Technologies” located two contracts (HSCETE11F00125 and HSCEMD11P0040) wherein ICE is assigned as the contracting agency. As described in paragraph 5 above, these two contracts were found to be not responsive to the Plaintiff’s FOIA request. A search of FPDS using the term “Berico Technologies” located zero contracts wherein ICE is assigned as the contracting agency.

45. Within the ICE Privacy Office, the ICE Privacy Officer and two Privacy Compliance Specialists conducted a manual review of their paper files for records that would be responsive to the FOIA request. Each individual then conducted a search of their computer and e-mail files using the terms “social media”, “Facebook”, “LinkedIn”, “Twitter”, and “MySpace”. No responsive records were located.

46. In a memorandum dated October 6, 2011, the ICE FOIA Office informed the DHS FOIA Office that a search of ICE program offices for records that would be responsive to Plaintiff’s FOIA request had failed to locate or identify any records.

MGMT Processing of the FOIA Request

47. The Under Secretary for Management (MGMT) is responsible for budget, appropriations, expenditure of funds, accounting and finance; procurement; human resources and personnel; information technology systems; facilities, property, equipment, and other material resources; and identification and tracking of performance measurements relating to the responsibilities of the Department.

48. MGMT is responsible for ensuring that employees have clear responsibilities and

¹ <https://www.fpds.gov/>

means of communication with other personnel and management. An important resource for communications will be the office of the Chief Information Officer, who is responsible for maintaining the information technology necessary to keep the more than 170,000 employees of DHS connected to and fully a part of the goals and mission of the Department.

49. In a memorandum dated April 29, 2011, the DHS Privacy forwarded a copy of Plaintiff's April 12, 2011 FOIA request to the MGMT Front Office, which manages FOIA requests. DHS instructed the Front Office to conduct a search for responsive records within MGMT, to review any such records in accordance with the FOIA for the purpose of release recommendations, and to provide any such recommendations to the DHS FOIA Office for use in a consolidated response.

50. MGMT assigned FOIA case number MGMT11-114 to the Plaintiff's FOIA request.

51. Upon MGMT's review of Plaintiff's FOIA request, the Front Office determined that the program offices most likely to maintain records that would be responsive to the Plaintiff's FOIA request were the Chief Information Officer (OCIO) and Office of Procurement Operations (OPO).

52. OCIO conducted a search of the computer systems SOC On-Line and Security Incident Database. The used the search terms "social media monitoring" and "media monitoring." No responsive records were located.

53. OPO conducted a search of the computer system PRISM in which contracts reside. Although they found records related to two of the companies named in the FOIA request, none of those records related to social media. No responsive records were located.

54. By email dated May 6, 2011, MGMT informed DHS Privacy that a search of MGMT

program offices for records that would be responsive to Plaintiff's FOIA request had failed to locate or identify any records.

USCG Processing of the FOIA Request

55. The U.S. Coast Guard is one of the five armed forces of the United States and the only military organization within the Department of Homeland Security. The Coast Guard mission is to safeguard our Nation's maritime interests and environment around the world.

56. The Chief, Management Programs and Policy Division oversees comprehensive Information Management (IM) policies/procedures encompassing myriad programs in conformance with System Development Lifecycle (SDLC) and Enterprise Architecture (EA) principles, including Freedom of Information (FOIA).

57. In a memorandum dated April 29, 2011, the DHS Privacy forwarded a copy of Plaintiff's April 12, 2011 FOIA request to the USCG FOIA Office. DHS instructed the USCG FOIA Office to conduct a search for responsive records within USCG, to review any such records in accordance with the FOIA for the purpose of release recommendations, and to provide any such recommendations to the DHS FOIA Office for use in a consolidated response.

58. USCG assigned FOIA case number USCG2012-0180 to the Plaintiff's FOIA request.

59. Upon review of Plaintiff's FOIA request, the USCG FOIA Office determined that the program office most likely to maintain records that would be responsive to the Plaintiff's FOIA request were the Coast Guard Office of Public Affairs (CG-0922) and the Coast Guard Office of Intelligence.

60. The Office of Public Affairs conducted a search of electronic and email files and no

responsive records were located.

61. The Coast Guard Office of Intelligence searched their electronic databases and email files and no responsive records were located.

61. By email dated January 13, 2012, the USCG FOIA Office informed DHS Privacy that a search of program offices for records that would be responsive to Plaintiff's FOIA request had failed to locate or identify any records.

FOIA EXEMPTIONS

63. In accordance with the requirements set forth in *Vaughn v. Rosen*, 484 F.2d 820 (D.C. Cir. 1973), this declaration provides an explanation of the basis for withholding portions of documents released to plaintiffs in the First Interim Release (January 10, 2011) and the Second Interim Release (DHS provided to DOJ on February 6, 2011), pursuant to FOIA Exemptions (b)(2)(high), (b)(5), (b)(6), (b)(7)(C), and (b)(7)(E).

64. The rationale of the DHS FOIA Office for withholding each particular category of information is set forth below, and in the accompanying *Vaughn* Index (**Exhibit A**).

65. On January 10, 2012, DHS Privacy issued its first interim response to EPIC. DHS Privacy indicated that it had completed its review of 341 pages. Of those pages, DHS Privacy determined that 175 pages of the records were releasable in their entirety, 110 pages were partially releasable, and 56 pages were withheld in their entirety pursuant to Title 5 U.S.C. § 552 (b)(3), (b)(4), (b)(5), (b)(6), (b)(7)(C), and (b)(7)(E), FOIA Exemptions 3,4,5,6, 7(C), and 7(E).

66. On February 6, 2012, DHS Privacy completed its second interim response which consisted of an additional 39 pages. Of those pages, DHS Privacy determined that 24 pages of the records were releasable in their entirety, and 15 pages are partially releasable pursuant to Title 5 U.S.C. § 552 (b)(6), (b)(7)(C), and (b)(7)(E), FOIA Exemptions 6, 7(C) and 7(E). DHS Privacy transmitted this response directly to the Department of Justice (DOJ) for handling in

light of the current litigation. As far as DHS Privacy is aware, the second interim response was provided to EPIC by DOJ on February 15, 2012.

67. **FOIA Exemption 4**: Exemption 4, 5 U.S.C. § 522(b)(4), protects "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential."

68. DHS asserted the (b)(4) exemption for certain commercial information contained in contract documents that is protected by trade secret and commercial or financial information obtained from a person that is privileged or confidential.

69. **FOIA Exemption 5**: Exemption 5, 5 U.S.C. § 522(b)(5), allows for the withholding of intra-agency documents that are normally privileged in the civil discovery context.

70. The deliberative process privilege protects the integrity of the deliberative or decision-making processes within the agency by exempting from mandatory disclosure opinions, conclusions, and recommendations included within interagency or intra-agency memoranda or letters. The release of this internal information would discourage the expression of candid opinions and inhibit the free and frank exchange of information among agency personnel.

71. DHS applied Exemption 5 to protect internal agency deliberative information and guidance regarding the use of social media to facilitate collaboration and information sharing inside and outside the agency as well as a draft memorandum analyzing guidelines for use of Remote Retrievable Disposable Desktop (RRDD).

72. **FOIA Exemption 6**: Exemption 6, 5 U.S.C. § 522(b)(6), permits the withholding of all information about individuals in "personnel and medical files and similar files" when the disclosure of such information "would constitute a clearly unwarranted invasion of personal privacy." When applying this exemption, the agency must balance the individual's personal

privacy interest against the public need for purposes of shedding light on the agency's performance of its statutory duties.

73. **FOIA Exemption 7(c)**: Exemption 7(c), 5 U.S.C. § 522(b)(6), Exemption 7(C) provides protection for personal information in law enforcement records.

74. DHS applied Exemption 6 and 7(C) to withhold names, phone numbers, and email addresses of federal and state employees and other third parties appearing in agency records.

75. Names and identifying information relating to third parties would not shed light on how the agency carried out its statutory responsibilities. To reveal the names and/or identifying information of third party individuals in the context of these records could reasonably be expected to cause embarrassment and humiliation, and thus constitutes a clearly unwarranted invasion of personal privacy. It could also result in their being contacted by the media or others seeking information about social media matters. Based upon the traditional recognition of strong privacy interests in law enforcement records, categorical withholding of information that identifies third parties in law enforcement records is appropriate. Moreover, the third parties identified in these records have not provided consent to the release of their personally identifying information.

76. Likewise, Exemptions 6 and 7(C) were applied in connection with the identities, email addresses, telephone numbers of government personnel. As agency employees carrying out actions that at times may be unpopular with certain sectors of the public, these employees could be subject to harassment and attempts by members of the public who disagree with agency actions, resulting in inference with these employees' performance of their official duties. Specific knowledge of the identities of those employees would not provide additional insight as to how the agency has carried out its statutory mandates.

77. **FOIA Exemption 7(e)**: Exemption 7(e), 5 U.S.C. § 522(b)(6), Exemption 7(E) affords protection to all law enforcement information that 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.”

78. DHS asserted the (b)7(e) redaction to protect records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions. Specifically, DHS determined that disclosure of law enforcement systems access checklists including passwords, code and other access information could reasonably be expected to risk circumvention of the law. This information is contained within checklists that are used as tools for the user to access the databases and law enforcement computer system(s) being used. DHS determined that disclosure of law enforcement systems access checklists could reasonably be expected to risk circumvention of the law since the disclosure of this information would allow unauthorized access to intelligence information which could result in tampering or other manipulation of information which could inhibit investigative efforts.

79. **Segregability**: Under FOIA, “any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt.” 5 U.S.C. § 552(b). DHS has reviewed each record released responsive to plaintiffs’ FOIA request to identify information exempt from disclosure or for which a discretionary waiver of exemption could be applied, and to determine which category of record(s) each document should be placed in the accompanying *Vaughn* index.



80. With respect to the records that were released in part, all information not

exempted from disclosure pursuant to the FOIA exemptions specified above was segregated and non-exempt portions released. Information withheld was individually determined to be exempt from release. To the extent records were withheld in their entirety, because the exempt information was so inextricably intertwined with the non-exempt information, if any, no portion of those records could be reasonably segregated and disclosed. To the extent a small number of non-exempt words or phrases were dispersed throughout the withheld information, those words and phrases, if disclosed, would be meaningless and would not serve the purpose of FOIA-to open agency action to the light of public scrutiny.

JURAT CLAUSE

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

Executed this 31st day of July, 2012.


James V.M.L. Holzer, 

Vaughn Index

Electronic Privacy Information Center v. United States Department of Homeland Security
Civil Action No. 11-2261

This Vaughn Index includes descriptions of the following document productions:

First Interim Response

[1] Contract Docs from OPS	Total Pages: 100	Page 2
[2] SNMC Analyst Handbook	Total Pages: 107	Page 5
[3] SNMC Policy Resources	Total Pages: 27	Page 6
[4] SNMC OPS	Total Pages: 60	Page 7
[5] USCIS Documents	<u>Total Pages: 46</u>	Page 12

Total Pages: 340

Second Interim Response

[6] Analysts Desk Binder	<u>Total Pages: 39</u>	Page 18
--------------------------	------------------------	---------

Total Pages: 39

KEY:

WIF: Withheld in Full

RIF: Released in Full

PR: Partially Released/Partially Redacted

FIRST INTERIM RESPONSE				
341 Pages Total				
DOCUMENT DESCRIPTION	PAGES	EXEMPTION/ STATUS	JUSTIFICATION/DESCRIPTION	REDACTION CATEGORY
[1] CONTRACT DOCUMENTS FROM OPS (See breakdown below)	100 Pages Total			
DHS Office of Procurement Operations Agreement/Contract number HSHQDC-10-00080 awarded to General Dynamic Advanced Information Systems effective 12/15/2010 Task/Delivery Order	7 Pages Total 4 RIF 3 PR	FOIA Exemption b(6)	This document is part of a contract processing file. DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.	PII
Solicitation/Contract/Order for Commercial Item Contract No GS-10F-0237L	14 Pages Total 6 RIF 8 PR	FOIA Exemptions b(4), b(6)	This document is part of a contract processing file. DHS applied the (b)(4) exemption by redacting the commercial information protected by trade secret and commercial or financial information obtained from a person that is privileged or confidential. This document is part of a contract processing file. DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal identifiable information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.	PII Commercial Information
Attachment 1 Statement of Work	11 Pages RIF	NA	This document is part of a contract processing file. NA	

Determination and Findings	2 Pages Total 1 RIF 1 PR	FOIA Exemptions b(6)	This document is part of a contract processing file. DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.	PII
Determination and Findings GS-10F-0237L/ HSHQDC-10-F-00080	3 Pages Total 1 RIF 2 PR	FOIA Exemptions b(6)	This document is part of a contract processing file. DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.	PII
Sample: Proposal Evaluation Plan	3 Pages Total 2 RIF 1 PR	FOIA Exemptions b(4)	This document is part of a contract processing file. DHS applied the (b)(4) exemption by redacting the commercial information protected by trade secret and commercial or financial information obtained from a person that is privileged or confidential.	Commercial Information
Unit Price	1 Page Total 1 PR	FOIA Exemptions b(4)	This document is part of a contract processing file. DHS applied the (b)(4) exemption by redacting the commercial information protected by trade secret and commercial or financial information obtained from a person that is privileged or confidential.	Commercial Information
Market Research Report	8 Pages Total 6 RIF 2 PR	FOIA Exemptions b(6)	This document is part of a contract processing file. DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.	PII
Attachment 1 Statement of Work	5 Pages RIF	NA	This document is part of a contract processing file. NA	

Requisition	2 pages PR	FOIA Exemptions b(6)	This document is part of a contract processing file. DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.	PII
Solicitation/Contract/Order for Commercial Item Solicitation Number HSHQDC-10-Q-00005	20 Pages Total 13 RIF 7 PR	FOIA Exemptions b(6)	This document is part of a contract processing file. DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.	PII
Attachment 1 Statement of Work	11 Pages RIF	NA	NA	
Past Performance Questionnaire HSHQDC-10-Q-00005	5 Pages PR	FOIA Exemptions b(6)	This document is part of a contract processing file. DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.	PII

<p>Award Decision Memorandum RFQ HSHQDC-10-Q-00005</p>	<p>4 Pages PR</p>	<p>FOIA Exemptions b(3), b(4), b(6)</p>	<p>This document is part of a contract processing file. DHS applied the (b)(3) exemption by redacting contract information pursuant to Section 253b(m) of Title 41, United States Code, which prohibits the release of any competitive proposal under the FOIA, except for those portions of the proposal set forth or incorporated by reference in a government contract. Since the statute leaves the agency with no discretion, DHS determined that all sections of the contractor proposal which were required to be submitted, and which were not incorporated into the contract, must be withheld under subsection (b)(3) of the FOIA.</p> <p>This document is part of a contract processing file. DHS applied the (b)(4) exemption by redacting the commercial information protected by trade secret and commercial or financial information obtained from a person that is privileged or confidential.</p> <p>This document is part of a contract processing file. DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.</p>	<p>PII</p>
<p>Determination and Findings GS-10F-0237L/HSHQDC-10-F-00080</p>	<p>4 Pages PR</p>	<p>FOIA Exemptions b(6)</p>	<p>This document is part of a contract processing file. DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.</p>	<p>PII</p>

<p>[2] Social Networking/Media Capability Analyst Handbook February 2010</p>	<p>107 Pages Total 22 WIF (pp 22-43) 69 RIF 16 PR</p>	<p>FOIA Exemptions b(5), b(6), b7(c), b7(e)</p>	<p>This document is an internal handbook providing reference material and guidance regarding how the Office of Operations Coordination and Planning (OPS), National Operations Center (NOC), will engage in social media monitoring and situational awareness.</p> <p>DHS applied the (b)(5) exemption by withholding in full the entire 22 pages of the Draft Concept of Operations (CONOPS) Social Networking/Media Capability Version 2.2 February 23, 2010 contained in the internal handbook. The CONOPS is a document describing the characteristics of the proposed system from the viewpoint of the users of the system.</p> <p>The document is deliberative because it is a draft document that is predecisional. The information in the document reflects the opinions of the agency employees involved in developing the proposed system. The release of this internal information would discourage the expression of candid opinions and inhibit the free and frank exchange of information among agency personnel.</p>	<p>PII; Deliberative Draft; Law enforcement investigative procedures (personal privacy); Law enforcement investigative procedures (disclose techniques and/or procedures for law enforcement investigations)</p>
-------------------------------------------------------------------------------------	-------------------------------------------------------------------	-------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>[2] Social Networking/Media Capability Analyst Handbook February 2010 (continued)</p>	<p>107 Pages Total 22 WIF (pp 22-43) 69 RIF 16 PR</p>	<p>FOIA Exemptions b(5), b(6), b7(c), b7(e)</p>	<p>DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.</p> <p>DHS applied the 7(C) exemption by redacting to the names of law enforcement personnel, email tracking information, and other contact information, the release of which could reasonably be expected to constitute an unwarranted invasion of personal privacy. Based upon the traditional recognition of strong privacy interest in law enforcement records, categorical withholding of information that identifies third parties in law enforcement records is ordinarily appropriate. As such, DHS determined that the privacy interest in the identities of individuals in the records requested clearly outweigh any minimal public interest in disclosure of the information.</p> <p>DHS applied the 7(E) exemption by redacting law enforcement passwords, codes and other access information. This information is contained within checklists that are used as tools for the user to access the databases and law enforcement computer system(s) being used. DHS determined that disclosure of law enforcement systems access checklists could reasonably be expected to risk circumvention of the law since the disclosure of this information would allow unauthorized access to intelligence information which could result in tampering or other manipulation of information which could inhibit investigative efforts.</p>	
-------------------------------------------------------------------------------------------------	-------------------------------------------------------------------	-------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

			<p>OPS and the NOC collect records in systems used for domestic situational awareness, law enforcement, intelligence, emergency response, private sector, and open-source reporting purposes. Many of the records maintained by OPS and the NOC are compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions.</p>	
<p>[3] Social Networking/Media Capability Resources for Privacy Issues February 2010 and Sensitive Systems Handbook v.2 Draft January 7, 2010</p>	<p>27 Pages Total 1 Page RIF 26 Pages WIF</p>	<p>FOIA Exemptions b(5)</p>	<p>This document is an internal draft handbook regarding how the Office of Operations Coordination and Planning (OPS), National Operations Center (NOC), will engage in social media monitoring and situational awareness.</p> <p>DHS applied the (b)(5) exemption to protect internal agency deliberative information related to the development and use of procedures, including technical specifications. Specifically, the document explores how the Office of Operations Coordination and Planning (OPS), National Operations Center (NOC), will engage in social media monitoring and situational awareness to assist the Department of Homeland Security (DHS) and its components involved in fulfilling OPS statutory responsibility (Section 515 of the Homeland Security Act (6 U.S.C. § 321d(b)(1)) to provide situational awareness and establish a common operating picture for the federal government, and for those state, local, and tribal governments, as appropriate. While this initiative is not designed to actively collect Personally Identifiable Information (PII), an analysis was conducted to determine the impact of collecting and disseminating PII for certain narrowly tailored categories (i.e., extremis situation involving potential life and death)</p>	<p>Deliberative draft;</p>

<p>[4] SNMC OP (See breakdown below)</p>	<p>60 Pages Total</p>		<p>These documents contain internal guidance and training resources regarding how the Office of Operations Coordination and Planning (OPS), National Operations Center (NOC), will engage in social media monitoring and situational awareness</p>	
<p>Social Network/Media Capability (SNMC) Battle Rhythm Version 11 23 March 2011</p>	<p>17 Pages Total 12 RIF 5 PR</p>	<p>FOIA Exemptions b(6), b7(e)</p>	<p>DHS applied the (b)(6) exemption the names of law enforcement personnel , email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.</p> <p>DHS applied the 7(E) exemption by redacting law enforcement passwords, codes and other access information. This information is contained within checklists that are used as tools for the user to access the databases and law enforcement computer system(s) being used. DHS determined that disclosure of law enforcement systems access checklists could reasonably be expected to risk circumvention of the law since the disclosure of this information would allow unauthorized access to intelligence information which could result in tampering or other manipulation of information which could inhibit investigative efforts.</p> <p>OPS and the NOC collect records in systems used for domestic situational awareness, law enforcement, intelligence, emergency response, private sector, and open-source reporting purposes. Many of the records maintained by OPS and the NOC are compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions.</p>	<p>PII; Law enforcement investigative procedures (disclose techniques and/or procedures)</p>

Draft Inadvertent PII Inclusion Procedure (External)	2 Pages PR	FOIA Exemptions b(6)	DHS applied the (b)(6) exemption by redacting names of law enforcement personnel , email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.	PII
Inadvertent PII Inclusion Procedure (Internal)	1 Page PR	FOIA Exemptions b(6)	DHS applied the (b)(6) exemption by redacting names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.	PII
New PIA Revisions 7 Jan11	2 Pages Total 1 RIF 1 PR	FOIA Exemptions b(6)	DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.	PII
NOC Media Monitoring Capability Privacy Proficiency Exam (Answer Key)	7 Pages RIF	NA	NA	

<p>MMC-SN Overarching PIA Implementation CONOPS</p>	<p>3 Pages Total 1 RIF 2 PR</p>	<p>FOIA Exemptions b(6), b7(e)</p>	<p>DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.</p> <p>DHS applied the 7(E) exemption by redacting law enforcement passwords, codes and other access information. This information is contained within checklists that are used as tools for the user to access the databases and law enforcement computer system(s) being used. DHS determined that disclosure of law enforcement systems access checklists could reasonably be expected to risk circumvention of the law since the disclosure of this information would allow unauthorized access to intelligence information which could result in tampering or other manipulation of information which could inhibit investigative efforts. OPS and the NOC collect records in systems used for domestic situational awareness, law enforcement, intelligence, emergency response, private sector, and open-source reporting purposes. Many of the records maintained by OPS and the NOC are compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions.</p>	<p>PII Law enforcement investigative procedures (disclose techniques and/or procedures)</p>
-----------------------------------------------------	-----------------------------------------	----------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------

SNMC Training Plan Version 1 March 2011	12 Pages Total 4 RIF 8 PR	FOIA Exemptions b(6), b7(e)	<p>DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.</p> <p>DHS applied the 7(E) exemption by redacting law enforcement passwords, codes and other access information. This information is contained within checklists that are used as tools for the user to access the databases and law enforcement computer system(s) being used. DHS determined that disclosure of law enforcement systems access checklists could reasonably be expected to risk circumvention of the law since the disclosure of this information would allow unauthorized access to intelligence information which could result in tampering or other manipulation of information which could inhibit investigative efforts. OPS and the NOC collect records in systems used for domestic situational awareness, law enforcement, intelligence, emergency response, private sector, and open-source reporting purposes. Many of the records maintained by OPS and the NOC are compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions.</p>	PII Law enforcement investigative procedures (disclose techniques and/or procedures)
Interim Guidance Regarding PII and Reference to Government Spokespersons and Non-US Citizen Terrorist or DTO Leaders Mon 8/30/2010	1 Page PR	FOIA Exemptions b(6)	DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.	PII

Interim MMC Personal Identifiable Information (PII) Guidance Thu 9/2/2010	2 Pages Total 1 RIF 1 PR	FOIA Exemptions b(6)	DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.	PII
Interim MMC Personal Identifiable Information (PII) Guidance Thu 9/3/2010	2 Pages 1 RF 1 PR	FOIA Exemptions b(6)	DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.	PII
COP Update change due to PII rules Thu 9/30/2010 12:19 PM	1 Page PR	FOIA Exemptions b(6)	DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel , email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.	PII

<p>MMC Application Training and Implementation Timeline</p>	<p>2 Pages PR</p>	<p>FOIA Exemptions b(6), b7(e)</p>	<p>DHS applied the (b)(6) exemption by redacting to the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.</p> <p>DHS applied the 7(E) exemption by redacting law enforcement passwords, codes and other access information. This information is contained within checklists that are used as tools for the user to access the databases and law enforcement computer system(s) being used. DHS determined that disclosure of law enforcement systems access checklists could reasonably be expected to risk circumvention of the law since the disclosure of this information would allow unauthorized access to intelligence information which could result in tampering or other manipulation of information which could inhibit investigative efforts. OPS and the NOC collect records in systems used for domestic situational awareness, law enforcement, intelligence, emergency response, private sector, and open-source reporting purposes. Many of the records maintained by OPS and the NOC are compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions.</p>	<p>PII Law enforcement investigative procedures (disclose techniques and/or procedures)</p>
-------------------------------------------------------------	-------------------	------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------

<p>VERSION 2 Updated Guidance to: MMC Watch Standers and Senior Reviewers to Increase the Focus on Operationally Valuable Media Reporting</p>	<p>7 Pages Total 5 RIF 2 PR</p>	<p>FOIA Exemptions b(6), b7(e)</p>	<p>DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.</p> <p>DHS applied the 7(E) exemption by redacting law enforcement passwords, codes and other access information. This information is contained within checklists that are used as tools for the user to access the databases and law enforcement computer system(s) being used. DHS determined that disclosure of law enforcement systems access checklists could reasonably be expected to risk circumvention of the law since the disclosure of this information would allow unauthorized access to intelligence information which could result in tampering or other manipulation of information which could inhibit investigative efforts. OPS and the NOC collect records in systems used for domestic situational awareness, law enforcement, intelligence, emergency response, private sector, and open-source reporting purposes. Many of the records maintained by OPS and the NOC are compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions.</p>	<p>PII Law enforcement investigative procedures (disclose techniques and/or procedures)</p>
<p>Exercises</p>	<p>1 Page PR</p>	<p>FOIA Exemptions b(6)</p>	<p>DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.</p>	<p>PII</p>

<p>Various emails beginning with Wednesday, April 22, 2009 10:28pm re Access to Open Source Information</p>	<p>32 Pages Total 2 RIF 30 PR</p>	<p>FOIA Exemptions b(6), b7(c)</p>	<p>These documents are internal-agency emails between OPS program officials. These emails contain information regarding the use of social media information, including information compiled for law enforcement purposes and/or information regarding law enforcement procedures.</p> <p>DHS applied the (b)(6) exemption by redacting to the names of law enforcement personnel, email tracking information, and other contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.</p> <p>DHS applied the 7(C) exemption by redacting the names of law enforcement personnel, email tracking information, and other contact information, the release of which could reasonably be expected to constitute an unwarranted invasion of personal privacy. Based upon the traditional recognition of strong privacy interest in law enforcement records, categorical withholding of information that identifies third parties in law enforcement records is ordinarily appropriate. As such, DHS determined that the privacy interest in the identities of individuals in the records requested clearly outweigh any minimal public interest in disclosure of the information.</p>	<p>PII; Law enforcement investigative procedures (personal privacy)</p>
-------------------------------------------------------------------------------------------------------------	-------------------------------------------	----------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------

DOCUMENT DESCRIPTION	PAGES	EXEMPTION/ STATUS	JUSTIFICATION/DESCRIPTION	REDACTION CATEGORY
[5] USCIS Documents (See breakdown below)	46 Pages Total			
September 00, 2009 Draft Memorandum Re Guidelines for Use of Remote Retrievable Disposable Desktop (RRDD)	2 Pages Total 2 WIF	FOIA Exemptions b(5)	This document is a draft memorandum analyzing guidelines for use of Remote Retrievable Disposable Desktop (RRDD). DHS applied the (b)(5) exemption to protect internal agency deliberative information related to the development and use of procedures related to Remote Retrievable Disposable Desktop.	Deliberative draft;

<p>Email chain Thursday, May 7, 2009 7:10pm re DHS Open Source Response to DHS RFI-461-CR-09-CIS</p>	<p>20 Pages PR</p>	<p>FOIA Exemptions b(6), b7(c)</p>	<p>These documents are internal-agency emails between OPS program officials. These emails contain information regarding the use of social media information, including information compiled for law enforcement purposes and/or information regarding law enforcement procedures.</p> <p>DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel , email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.</p> <p>DHS applied the 7(C) exemption by redacting the names of law enforcement personnel, email tracking information, and other contact information, the release of which could reasonably be expected to constitute an unwarranted invasion of personal privacy.</p> <p>Based upon the traditional recognition of strong privacy interest in law enforcement records, categorical withholding of information that identifies third parties in law enforcement records is ordinarily appropriate. As such, DHS determined that the privacy interest in the identities of individuals in the records requested clearly outweigh any minimal public interest in disclosure of the information.</p>	<p>PII; Law enforcement investigative procedures (personal privacy;</p>
----------------------------------------------------------------------------------------------------------------------	--------------------	--------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------

<p>DHS Intelligence RFI Submission Form</p>	<p>3 Pages</p>	<p>FOIA Exemptions b(6), b7(c)</p>	<p>This document is an internal reporting form for intelligence information.</p> <p>DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.</p> <p>DHS applied the 7(C) exemption by redacting to the names of law enforcement personnel, email tracking information, and other contact information, the release of which could reasonably be expected to constitute an unwarranted invasion of personal privacy.</p> <p>Based upon the traditional recognition of strong privacy interest in law enforcement records, categorical withholding of information that identifies third parties in law enforcement records is ordinarily appropriate. As such, DHS determined that the privacy interest in the identities of individuals in the records requested clearly outweigh any minimal public interest in disclosure of the information.</p>	<p>PII; Law enforcement investigative procedures (personal privacy);</p>
---------------------------------------------	----------------	------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------

<p>Email May 21, 2008 Re Social Networking Sites</p>	<p>1 Page</p>	<p>FOIA Exemptions b(6), b7(c)</p>	<p>These documents are internal-agency emails between OPS program officials. These emails contain information regarding the use of social media information, including information compiled for law enforcement purposes and/or information regarding law enforcement procedures.</p> <p>DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel , email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.</p> <p>DHS applied the 7(C) exemption by redacting to the names of law enforcement personnel, email tracking information, and other contact information, the release of which could reasonably be expected to constitute an unwarranted invasion of personal privacy.</p> <p>Based upon the traditional recognition of strong privacy interest in law enforcement records, categorical withholding of information that identifies third parties in law enforcement records is ordinarily appropriate. As such, DHS determined that the privacy interest in the identities of individuals in the records requested clearly outweigh any minimal public interest in disclosure of the information.</p>	<p>PII; Law enforcement investigative procedures (personal privacy;</p>
--------------------------------------------------------------	---------------	--------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------

<p>Social Networking Sites and Their Importance to FDS</p>	<p>5 Pages Total 2 RIF 3 WIF</p>	<p>FOIA Exemptions b(6), b7(c)</p>	<p>This document is an internal information memo providing background and resources relevant to the use of social networking sites for the detection of fraud.</p> <p>DHS applied the (b)(6) exemption by redacting the names of lower level employees, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.</p> <p>DHS applied the 7(C) exemption by redacting to the names of law enforcement personnel, email tracking information, and other contact information, the release of which could reasonably be expected to constitute an unwarranted invasion of personal privacy.</p> <p>Based upon the traditional recognition of strong privacy interest in law enforcement records, categorical withholding of information that identifies third parties in law enforcement records is ordinarily appropriate. As such, DHS determined that the privacy interest in the identities of individuals in the records requested clearly outweigh any minimal public interest in disclosure of the information.</p>	<p>PII; Law enforcement investigative procedures (personal privacy;</p>
------------------------------------------------------------	------------------------------------------	----------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------

<p>Email chain October 26, 2009 re Anonymous Web Surfing and Open Source Unfettered Access</p>	<p>15 Pages 15 PR</p>	<p>FOIA Exemptions b(6), b7(c)</p>	<p>These documents are internal-agency emails between OPS program officials. These emails contain information regarding the use of social media information, including information compiled for law enforcement purposes and/or information regarding law enforcement procedures.</p> <p>DHS applied the (b)(6) exemption by redacting the names of law enforcement personnel, email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.</p> <p>DHS applied the 7(C) exemption by redacting to the names of law enforcement personnel, email tracking information, and other contact information, the release of which could reasonably be expected to constitute an unwarranted invasion of personal privacy.</p> <p>Based upon the traditional recognition of strong privacy interest in law enforcement records, categorical withholding of information that identifies third parties in law enforcement records is ordinarily appropriate. As such, DHS determined that the privacy interest in the identities of individuals in the records requested clearly outweigh any minimal public interest in disclosure of the information.</p>	<p>PII; Law enforcement investigative procedures (personal privacy)</p>
----------------------------------------------------------------------------------------------------------------	---------------------------	--------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------

SECOND INTERIM RESPONSE				
39 Pages Total				
DOCUMENT DESCRIPTION	PAGES	EXEMPTION/ STATUS	JUSTIFICATION/DESCRIPTION	REDACTION CATEGORY
[6] Analyst's Desktop Binder 2011: Department of Homeland Security National Operations Center Media Monitoring Capability Desktop Reference Binder (39 Total Pages)	39 Total Pages 24 Pages RIF 15 Pages PR	FOIA Exemptions b(6), (b)(7)(c) and b7(e)	<p>This document is a reference binder providing internal agency guidance regarding the use of social media to facilitate collaboration and information sharing inside and outside the agency.</p> <p>DHS applied the (b)(6) and (b)(7)(c) exemptions by redacting the names of law enforcement personnel , email tracking information, and other personal contact information. Releasing this information would constitute an unwarranted invasion of the individual's privacy.</p> <p>DHS applied the (b)(7)(e) exemption by redacting law enforcement passwords, codes and other access information that could reasonably be expected to risk circumvention of the law. This information is contained within checklists that are used as tools for the user to access the databases and law enforcement computer system(s) being used. DHS determined that disclosure of law enforcement systems access checklists could reasonably be expected to risk circumvention of the law since the disclosure of this information would allow unauthorized access to intelligence information which could result in tampering or other manipulation of information which could inhibit investigative efforts.</p>	PII; Deliberative draft; Predecisional Law enforcement investigative procedures (personal privacy); Law enforcement investigative procedures (disclose techniques and/or procedures for law enforcement investigations

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION)
CENTER)

Plaintiff,)

v.)

Civ. Action No. 1:11-cv-02261-JDB

UNITED STATES DEPARTMENT OF)
HOMELAND SECURITY,)

Defendant.)
_____)

DECLARATION OF JULIE FERRELL
ACTING SPECIAL AGENT IN CHARGE LIAISON DIVISION AND
ACTING FREEDOM OF INFORMATION ACT AND PRIVACY ACT OFFICER,
UNITED STATES SECRET SERVICE

I, Julie Ferrell, hereby make the following declaration:

1. I am the Acting Special Agent in Charge of the Liaison Division, Office of Government and Public Affairs and the Freedom of Information Act and Privacy Act (FOIA/PA) Officer for the United States Secret Service ("Secret Service"), Department of Homeland Security ("DHS"). I have been assigned as the Secret Service FOIA/PA Officer since May 23, 2012, and have been employed with the Secret Service as a Special Agent (GS-1811) since March 21, 1994.
2. DHS regulations, Title 6, Code of Federal Regulations, Section 5.4, and Appendix A, II(I)(3), 68 FR 4056, 4058, and 4069, vest authority in the Secret Service FOIA/PA Officer to make initial determinations as to whether to grant requests for access to Secret Service records made under the Freedom of Information Act ("FOIA"), Title 5

of the United States Code, Section 552(b).

3. The statements I make in this declaration are made on the basis of my personal knowledge or upon information acquired by me during the performance of my official duties.

The Receipt of Plaintiff's Requests

4. As the Secret Service's FOIA/PA Officer, I am familiar with the Plaintiff's FOIA request. The files of the Secret Service have been searched for records pertinent to the Plaintiff's FOIA request. A description of the processing of the Plaintiff's request is set forth below.
5. On January 12, 2012, the Secret Service FOIA/PA Office received an e-mail, from the DHS Privacy Office, notifying the Secret Service FOIA/PA Office that on December 21, 2011, the Plaintiff had filed the instant action against DHS claiming constructive denial and denial of their media status with respect to Plaintiff's April 19, 2011 FOIA request to DHS. DHS attached a copy of the Plaintiff's FOIA request to the e-mail and requested that the Secret Service search for materials responsive to the request.
6. The Plaintiff requested the following categories of agency records:
 - All contracts, proposals, and communications between the federal government and third parties, including but not limited to, H.B. Gary Federal, Palantir Technologies, and/or Berico Technologies, and/or parent or subsidiary companies, that include provisions concerning the capability of social media monitoring technology to capture, store, aggregate, analyze, and/or match personally-identifiable information.
 - All contracts, proposals, and communications between DHS and any states, localities, tribes, territories, and foreign governments, and/or their agencies or subsidiaries, and/or any corporate entities, including but not limited to H.B. Gary Federal, Palantir Technologies, and/or Berico Technologies, regarding the implementation of any social media monitoring initiative.

- All documents used by DHS for internal training of staff and personnel regarding social media monitoring, including any correspondence and communications between DHS, internal staff and personnel, and/or privacy officers, regarding the receipt, use, and/or implementation of training and evaluation documents.
- All documents detailing the technical specifications of social media monitoring software and analytic tools, including any security measures to protect records of collected information and analysis.
- All documents concerning data breaches of records generated by social media monitoring technology.

A copy of this e-mail and its attachments are attached as Exhibit A.

The Searches for Responsive Records

7. Upon review of the Plaintiff's FOIA request, the Secret Service FOIA/PA Office determined that in order to conduct as wide a search as was reasonably possible, the request would be sent to multiple divisions within the Secret Service to ascertain if they had potentially responsive records.
8. Based upon the subject matter of the request, the FOIA/PA office identified the following Secret Service divisions as those that may potentially have responsive records: the Office of Investigations ("INV"); the Criminal Investigative Division ("CID"); the Procurement Division ("PRO"); the James J. Rowley Training Center ("JJRTC"); the Office of Chief Counsel ("LEG"); the Information Resource Management Division ("IRMD"); and the Strategic Intelligence and Information Division ("SII").
9. INV was asked to search for responsive records because it has oversight over the criminal investigative responsibilities of the Secret Service, such as investigating violations of the laws of the United States relating to its currency and financial systems, as well as developing, recommending and implementing changes in Secret

Service enforcement programs, policies and procedures.

10. After a careful review of the Plaintiff's FOIA request and consulting the relevant subject-matter expert, INV determined that it was not involved in social media monitoring initiatives and, therefore, would not have responsive records. INV responded to the FOIA/PA Office search request on January 20, 2012, indicating no records were found.
11. CID was asked to search for documents because it is the division within the Secret Service that plans, reviews, and coordinates domestic and international criminal investigations, such as those involving the counterfeiting of U.S. coins and currency, identity crimes, and bank fraud. After reviewing the FOIA request, CID conducted an electronic database query and determined that it did not have responsive records concerning social media monitoring. CID responded to the FOIA/PA Office search request on January 26, 2012, indicating no records were found.
12. After the responsive materials received from the other divisions were reviewed, CID was asked to conduct an additional search for records responsive to the request. The request was referred to a subject matter expert within CID and that individual conducted an electronic search of his files, including e-mail, and located potentially responsive records. Those documents were forwarded to the FOIA/PA office for review and processing on June 30, 2012.
13. Given that the request asked for contracts and agreements, PRO was asked to search for responsive records. PRO is the contracting branch of the Secret Service and is responsible for the acquisition of all goods and services for the protective, investigative, and administrative missions of the Secret Service. Contracts entered

into by the Secret Service are held in the division.

14. PRO conducted an electronic search of an internal database, called PRISM, to determine if any relevant contract actions existed. PRISM contains, among other information, a record of all finalized contracts, as well as information on requests for certain proposals and requests for quotes that have been entered into the system. It is not possible to perform complex searches within the PRISM database. The ability, therefore, to search for general subject areas is extremely limited and burdensome. In an attempt to compensate for these technological limitations, PRO performed electronic queries using various terms including "Palantir Technologies", "Berico Technologies", and "media monitor". After reviewing the search results, PRO determined that one contract and one contract modification were potentially responsive to the request.
15. PRO responded to the FOIA/PA Office search request indicating that records were found and PRO forwarded those records for processing on June 4, 2012.
16. As the request asked for documents used for internal training of staff and personnel, the FOIA/PA Office also requested that JJRTC search for documents. JJRTC is the training branch of the Secret Service and develops and implements training programs, provides training for all Secret Service employees, and initiates long-range developmental training programs as necessary.
17. In responding to the request, JJRTC reviewed its electronic learning management system course catalogue to determine if any of its curricula and training materials related to the subject matter of the request. JJRTC also queried its supervisory employees in charge of the various training units of the division, and requested that

those individuals also search to determine if they held any potentially responsive records.

18. JJRTC determined that it maintained no records that specifically addressed social media monitoring training and, therefore, had no records potentially responsive to the Plaintiff's FOIA Request. JJRTC did locate training materials that addressed situational awareness initiatives in general and, even though these materials did not address social media monitoring, in an overabundance of caution, JJRTC nevertheless forwarded those documents to FOIA/PA for review on June 20, 2012.
19. LEG is responsible for providing legal advice and counsel on all programs and activities of the Secret Service including legal research, advice, and opinions on questions of constitutional law, ethics, procurement, the processing of records and adjudication of appeals pursuant to the FOIA/PA, the release of Secret Service records and information pursuant to Federal laws and regulations, and drafting and reviewing Secret Service and DHS policy and management directives.
20. After carefully reviewing the search request, LEG requested that all its employees search their records for potentially responsive materials. This request encompassed the attorneys who had previously worked on issues involving social media and who were, therefore, more likely to have potentially responsive records. Those attorneys conducted a manual review of their hard copy files, including case files, for records related to social media issues that would be responsive to the Plaintiff's FOIA request. Those individuals also reviewed and/or conducted electronic searches of their e-mail and electronic documents for potentially responsive records. Search terms used included terms such as "social media", "monitoring", "internet", and

“Facebook”. Potentially responsive records were located and forwarded to the FOIA/PA office for review on June 12, 2012.

21. The Plaintiff’s FOIA request sought records regarding the technological capabilities of social media monitoring technology; therefore, IRMD was asked to search for potentially responsive records. IRMD plans, designs, develops, operates, and manages information technology solutions to support the protective and investigative missions and associated administrative and management functions of the Secret Service.
22. After receiving and carefully reviewing the search request, IRMD consulted with the appropriate subject-matter experts within the division and determined that the division would not have any responsive records as it did not engage in the monitoring of social media. IRMD responded to the FOIA/PA Office search request indicating that no responsive records were located on February 18, 2012.
23. SII creates, establishes, and implements the strategic direction of the Protective Intelligence and Assessment Division (“PID”) in its operational efforts to collect, analyze, coordinate, investigate, implement and manage the operational intelligence and information affecting the protective mission of the Secret Service. After receiving and reviewing the request, a subject matter expert searched the appropriate SII files and located potentially responsive records. SII forwarded those potentially responsive records to the FOIA/PA office for review and processing on June 21, 2012.
24. SII also forwarded the FOIA request to PID, which provides guidance and coordinates all protective intelligence investigations and advances; analyzes,

evaluates, disseminates, and maintains information about individuals, groups, and activities that pose a potential threat to persons, facilities, and events protected by the Secret Service; and provides threat assessment briefings and other information pertinent to the protective intelligence mission of the Agency.

25. After receiving the request from SII, PID reviewed the request and then forwarded it to the appropriate subject matter expert in that office, who conducted an electronic search of PID's files, including e-mail, using keywords such as "social media." Potentially responsive records were located. SII then forwarded those records to the FOIA/PA office for review and processing on June 12, 2012.

Processing the Potentially Responsive Records

26. After reviewing the potentially responsive records received from JJRTC, LEG, CID, PID, PRO, and SII, it was determined that 365 pages of records from PRO, LEG, CID, PID and SII were responsive to the Plaintiff's request. These responsive records were then processed by the Secret Service FOIA/PA Office under the FOIA.
27. On July 2, 2012, the Secret Service informed the Plaintiff that it had not yet completed processing all of the records that were responsive to the Plaintiff's FOIA request but that the Agency was releasing those responsive records that the Secret Service had completed processing to date. That same day, the Agency released fifty-five pages of records with no exemptions claimed to the Plaintiff.
28. The Secret Service completed its review of the remaining records responsive to the Plaintiff's FOIA request on July 6, 2012. The review concluded that 32 additional pages of records should be released to the Plaintiff without redactions, that 48 pages of records should be released to the Plaintiff with redactions pursuant to FOIA

exemptions (b)(4), (b)(6), (b)(7)(C) and (b)(7)(E), and that 230 pages should be withheld in their entirety from the Plaintiff pursuant to FOIA exemptions (b)(4), (b)(5), (b)(6), (b)(7)(C) and (b)(7)(E).

29. On July 6, 2012, the Secret Service released to the Plaintiff 32 pages of records with no exemptions claimed, released 48 pages with exemptions claimed, and informed the Plaintiff that 230 pages of additional records were being withheld in their entirety.
30. A *Vaughn* index, attached to this declaration as Exhibit B, sets forth a description of those responsive records released with redactions or withheld in their entirety, identifies the type of information contained in those records, and identifies the exemptions invoked in withholding such information.

A. 5 U.S.C. 552(b)(4): Commercial or Financial Information

31. Title 5 of the United States Code, Section 552(b)(4), exempts from disclosure "trade secrets and commercial or financial information obtained from a person and privileged or confidential."
32. The Secret Service is invoking exemption (b)(4) to withhold the commercial and financial information contained in documents 1 to 6, 11, 14, 16, 17, 28, 29, 32, 33 and 35. These documents contain information regarding a company's pricing, technical specifications, and performance capabilities, prepared and submitted to the Secret Service in order to convince the Secret Service to award a contract to the provider. This type of information is not customarily disclosed to the public by the company and was provided with the expectation that it would not be disclosed outside of the government.
33. The release of this type of information would impair the ability of the government to

obtain necessary information from commercial suppliers and impact the accuracy and full availability of such information. For the reasons above, the Secret Service is withholding portions of documents 1 to 6, 11, 14, 16, 17, 32, 33 and 35 pursuant to exemption (b)(4).

B. 5 U.S.C. 552(b)(5): Inter-Agency Or Intra-Agency Material That Would Not Be Available In the Civil Discovery Process

34. Title 5 of the United States Code, Section 552(b)(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.” This exemption has been construed to cover those documents that are normally privileged in the civil discovery context.
35. The Secret Service is invoking exemption (b)(5) to withhold, in full, documents 7, 8 and 9. These documents contain factual information provided to Agency counsel by employees of PID and its contractor working within the Agency. This information was given by Agency to its counsel for the purpose of seeking legal advice regarding the requirements of an ongoing internal Agency project and the contractual obligations associated with that project. These documents also contain the legal advice provided by Agency counsel to the client based on those facts. This information, which has not been shared with third parties, is confidential communications between Agency counsel and their client. The release of this information would intrude upon the attorney-client relationship, discourage frank and open discussions between the Secret Service and agency counsel, and create a chilling effect that could harm the ability of Agency counsel to provide sound legal advice. Such a result could harm the protective efforts of the Secret Service. For the reasons

above, the Secret Service is withholding seven pages of records, pursuant to exemption (b)(5), in documents 7, 8 and 9.

C. 5 U.S.C. 552(b)(6) and (b)(7)(C): Records Or Information the Disclosure Of Which Would Be an Unwarranted Invasion Of Personal Privacy

36. Title 5, United States Code, Section 552(b)(6) exempts from disclosure “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.” Information that applies to or describes a particular individual qualifies as “personnel,” “medical,” or “similar files” under exemption (b)(6). This exemption protects both government officials and private third parties, whose identities are revealed in government records, from unwarranted invasions of their personal privacy that would not shed light on government activities.
37. Title 5, United States Code, Section 552(b)(7)(C) exempts from disclosure “records or information compiled for law enforcement purposes” the disclosure of which “could reasonably be expected to constitute an unwarranted invasion of personal privacy.” This exemption protects, among other information, the identity of law enforcement personnel and third parties referenced in files compiled for law enforcement purposes.
38. The Secret Service is a criminal law enforcement and security agency created under Title 18, United States Code, Section 3056. The files identified in response to the Plaintiff’s FOIA requests were compiled in connection with the Secret Service’s protective mission. These files were compiled under the authority to conduct such investigations as vested in the Secret Service under Title 18, United States Code, Section 3056. As such, these records meet the threshold requirement of exemption (b)(7) of having been compiled for law enforcement purposes.

39. The Secret Service is invoking exemptions (b)(6) and (b)(7)(C) to withhold the names, e-mail addresses and/or contact numbers of law enforcement personnel in documents 1 to 6, 9, 11, 12, 13, and 15 to 42. The identity of federal law enforcement personnel are withheld in order to avoid subjecting public servants to harassment and annoyance either in the conduct of their official duties or their private lives.
40. In making its determination to withhold the identities and telephone numbers of law enforcement personnel under exemptions (b)(6) and (b)(7)(C), the Secret Service balanced the public's interest in disclosure against the privacy rights of the individual whose names and telephone numbers appears in responsive documents. The Secret Service determined that there is no public interest in this information, since this information does not reveal anything about the manner in which the agency conducts its activities, nor does it disclose any illegal activity on the part of the agency. Moreover, the public interest is best served by the non-disclosure of such information, since disclosure could result in the personal harassment of law enforcement personnel and, by extension, a diminishment of the ability of law enforcement personnel to perform their duties. Furthermore, the performance of law enforcement duties often entails serious intrusions into the lives of others, which creates resentment and sometimes a desire for retaliation. As such, the Secret Service recognizes that the release of the names and telephone numbers of law enforcement personnel could facilitate such retaliation.
41. The Secret Service is also invoking exemptions (b)(6) and (b)(7)(C) to withhold the names, contact numbers, e-mail addresses, and other identifying information of third parties whose names and identifying information appear on these documents and who

provided information and/or services to the Secret Service in connection with its protective mission. The Secret Service has withheld such third party information in documents 1, 2, 3, 5, 6, 9 to 15, and 17 to 42.

42. In making its determination to withhold, under exemptions (b)(6) and (b)(7)(C), the names and other identifying information of third parties that appear in these documents, the Secret Service balanced the public's interest in disclosure against the rights of these third parties to personal privacy, and determined that the privacy rights of third parties outweighed any public interest in disclosure. The Secret Service determined that there is no public interest in the disclosure of third party names and identifying information, because such information reveals nothing about the manner in which the agency conducts its activities, nor does it disclose any illegal activity on the part of the agency. The Secret Service considered the potentially stigmatizing effect resulting from the appearance of third party names in law enforcement files. The Secret Service also recognized that disclosure of third party information might have the effect of chilling future cooperation by third parties with law enforcement agencies. The Secret Service is also particularly concerned with the protection of personal information of third parties because the agency's investigative mission include jurisdiction over identity crimes and fraud. Given these factors, the Secret Service determined that the privacy rights of third parties outweigh the public's interest in disclosure.

43. For the reasons above, the Secret Service is withholding portions of documents 1, 2, 3, 5, 6, 9 to 15, 17 to 22, 24 to 39, 41, and 42, and withholding in full one page (of the total two pages) in document 40, pursuant to exemptions (b)(6) and (b)(7)(C). The

Secret Service is also withholding in full twenty-four pages (of the total twenty-six pages) in document 23. These twenty-four pages consist of access forms that have been filled in by various individuals and contain such personally identifiable information as names, social security numbers, and dates of birth. If this personally identifiable information was redacted from the document, all that would remain would be empty standard forms. Therefore, the Secret Service is withholding these pages in full pursuant, to exemptions (b)(6) and (b)(7)(C).

D. 5 U.S.C. 552 (b)(7)(E): Records Or Information Which Would Disclose Techniques and Procedures For Law Enforcement Investigations Or Prosecutions

44. Title 5, United States Code, Section 552(b)(7)(E) exempts from disclosure “records or information compiled for law enforcement purposes” the disclosure of which “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.”
45. The Secret Service is invoking exemption (b)(7)(E) to withhold, in its entirety, the following: information on a technique utilized by the Secret Service in identifying, and analyzing potential threats against the President, Vice-President and other Secret Service protectees, the specific guidelines used to identify potential threats, and information regarding systems and technology used as part of that technique, including system configuration and information on system vulnerabilities. The Secret Service is using this exemption to withhold portions of documents 15, 18, 23, 26, 27, 28, 30, 32 to 35, 37 and 42; to withhold in full documents 1 to 11, 14, 16, 17, 19, and

20; and to withhold in full two pages (of the total three pages) in document 12, two pages (of the total three pages) in document 13, nineteen pages (of the total twenty pages) in document 21, and twelve pages (of the total thirteen pages) in document 22.

46. The release of this information would reveal the details of techniques and methodologies used by the Secret Service that are not generally known to the public. Public disclosure of information about how potential threats are identified and investigated could nullify the future effectiveness of these protective and investigative measures and render them operationally useless. Release of this information could benefit those attempting to harm Secret Service protectees by enabling them to thwart detection and avoid or hinder protective intelligence investigations. Disclosure of this type of information could impede the Secret Service's efforts to protect the President of the United States, the Vice-President, and other protectees in the future. For these reasons, the Secret Service is withholding, in full, 205 pages of material pursuant to exemption (b)(7)(E).

Segregation

47. Every effort has been made to provide the Plaintiff with all reasonably segregable portions of the material requested. The Secret Service has carefully reviewed the responsive records and has determined what portions must be released and what portions must be withheld. No reasonably segregable non-exempt portions of documents have been withheld from the Plaintiff.
48. A review of the responsive documents shows that no information can be segregated without releasing information properly withheld under the FOIA. If exempt information were redacted from the pages withheld in their entirety, the only

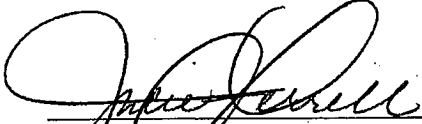
remaining information would be either meaningless and/or result in an essentially blank page. Accordingly, all information withheld is exempt from disclosure pursuant to FOIA exemptions (b)(4), (b)(5), (b)(6), (b)(7)(C), or (b)(7)(E), or is not reasonably segregable.

Conclusion

49. The Secret Service has released as much information as possible and has processed the documents to withhold only the information which it has determined can be withheld pursuant to valid FOIA exemptions and which must be withheld in order for the Secret Service to best perform its protective and investigative functions. The Secret Service has made every attempt to comply with the intent of the FOIA, while protecting confidential commercial and financial information, the personal privacy of third parties, the attorney-client privilege, and the interest of the general public in the efficient and effective performance of its law enforcement duties.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

31 July 2012
Date



Julie Ferrell
Acting Special Agent in Charge,
Acting Freedom of Information Act and
Privacy Act Officer
Liaison Division
United States Secret Service

VAUGHN DOCUMENT INDEX

Documents Potentially Responsive to Plaintiff's FOIA Request

Document 1, USSS-000001-10

Description

Two page letter and eight pages of attachments from an outside contractor dated April 6, 2009 to a Special Agent in the Protective Intelligence and Assessment Division providing a cost proposal, withheld in full.

Information Withheld/Exemption(s) claimed

(b)(7)(E)

Information regarding a system used to identify, analyze and investigate potential threats against Secret Service protectees.

(b)(6), (b)(7)(C)

Names of Secret Service personnel
Name, e-mail address and phone number of third party

(b)(4)

Proprietary and confidential company pricing information

Document 2, USSS-000011-13

Description

Three page draft version of April 6, 2009 letter, dated April 3, 2009 (document 1, above without attachments), withheld in full.

Information Withheld/Exemption(s) claimed

(b)(7)(E)

Information regarding a system utilized in identifying, analyzing, and investigating potential threats against Secret Service protectees.

(b)(6), (b)(7)(C)

Name of Secret Service personnel
Name, e-mail address and phone number of third party

(b)(4)

Proprietary and confidential company pricing information

Document 3, USSS-000014

Description

One page letter dated October 13, 2007 to a Special Agent in the Protective Intelligence and Assessment Division submitting a price quote, withheld in full.

Information Withheld/Exemption(s) claimed

(b)(7)(E)

Information regarding a system used to identify, analyze and investigate potential threats against Secret Service protectees, the details of which would disclose information about protective intelligence techniques.

(b)(6), (b)(7)(C)

Name of Secret Service personnel
Name, e-mail address, and phone number of third party

(b)(4)

Proprietary and confidential company pricing information

Document 4, USSS-000015-25

Description

Eleven page contract with an order date of March 28, 2007, withheld in full.

Information Withheld/Exemption(s) claimed

(b)(7)(E)

Descriptions of sensitive software modifications necessary for utilization in

protective intelligence operations and investigations.

(b)(6), (b)(7)(C)

Names and phone numbers of Secret Service personnel

(b)(4)

Company pricing information

Document 5, USSS-000026-47

Description

Nine page contract with an order date of March 19, 2008, and a thirteen page statement of work dated January 24, 2008, withheld in full.

Information Withheld/Exemption(s) claimed

(b)(7)(E)

Description of proposed modifications to Secret Service critical systems
Information on various Secret Service databases and details of system capabilities

(b)(6), (b)(7)(C)

Names and phone numbers of Secret Service personnel
Names, e-mail addresses and phone numbers of third parties

(b)(4)

Proprietary and confidential company commercial and financial information

Document 6, USSS-000048-69

Description

Seven page contract with an award date of July 27, 2009, and fifteen pages of associated documents, withheld in full.

Information Withheld/Exemption(s) claimed

(b)(7)(E)

Information regarding a system used to identify, analyze and investigate potential threats against Secret Service protectees, the details of which would disclose information about protective intelligence techniques.

(b)(6), (b)(7)(C)

Names and phone numbers of Secret Service personnel
Name, e-mail address and phone number of third party

(b)(4)

Proprietary and confidential company commercial and financial information

Document 7, USSS-000070

Description

One page of attorney handwritten notes from a January 7, 2011 meeting with representatives from the Protective Intelligence and Assessment Division and the contractor, withheld in full.

Information Withheld/Exemption(s) claimed

(b)(7)(E)

Information regarding data retention capabilities of a system utilized in identifying and analyzing threats against Secret Service protectees, the disclosure of which would reveal details regarding the protective intelligence technique.

(b)(5)

Information reflecting attorney-client privileged communications regarding legal implications of data retention.

Document 8, USSS-000071-74

Description

Four pages of attorneys' handwritten notes from a March 4, 2011 meeting with Agency stakeholders and contractor representatives regarding contract modifications, withheld in full.

Information Withheld/Exemption(s) claimed

(b)(7)(E)

Information regarding data retention capabilities of a system utilized in identifying and analyzing threats against Secret Service protectees, the disclosure of which would reveal details regarding the protective intelligence technique.

(b)(5)

Information reflecting attorney-client privileged communications regarding the legal implications of data retention.

Document 9, USSS-000075-76

Description

January 2011 e-mails between Agency counsel and Protective Intelligence and Assessment Division employees reflecting follow-up conversations following January 7, 2011 meeting, withheld in full.

Information Withheld/Exemption(s) claimed

(b)(5)

Information reflecting attorney-client privileged communications regarding the legal implications of data retention.

(b)(7)(E)

Information regarding data retention and reporting capabilities of a system utilized in identifying and analyzing threats against Secret Service protectees, the disclosure of which would reveal details regarding the protective intelligence technique.

(b)(6), (b)(7)(C)

Names of Secret Service personnel
Names of third parties

Document 10, USSS-000077-98

Description

Twenty-two page power point presentation dated January 2010 prepared for the Secret Service by a third party, withheld in full.

Information Withheld/Exemption(s) claimed

(b)(7)(E)

The details regarding system to be utilized in identifying, analyzing, and investigating threats against Secret Service protectees, including its functionality, the disclosure of which would reveal details about protective intelligence techniques.

(b)(6), (b)(7)(C)

Name, e-mail address and phone number of third party

Document 11, USSS-000099-102

Description

Four page proposal dated March 4, 2011, prepared for the Secret Service by contractor regarding proposed contract modifications, withheld in full.

Information Withheld/Exemption(s) claimed

(b)(7)(E)

Description of proposed modifications to a system utilized in identifying, analyzing, and investigating threats against Secret Service protectees, the disclosure of which would reveal details about protective intelligence techniques.

(b)(6), (b)(7)(C)

Name of Secret Service personnel
Names of third parties

(b)(4)

Proprietary and confidential price analysis of proposed modifications.

Document 12, USSS-000103-105

Description

A September 2011 e-mail chain involving Agency employees and contractor, released with redactions; an attached two-page contract modification, withheld in full.

Information Withheld/Exemption(s)

(b)(7)(E)

Information regarding a system used to identify, analyze, and investigate threats against Secret Service protectees, the identity of which would disclose details about protective intelligence techniques.

(b)(6), (b)(7)(C)

Names, e-mail address, signature, and phone number of Secret Service personnel
Name of third party

Document 13, USSS-000106-108

Description

A September 2011 e-mail from a contractor to an Agency employee (a reply to document 12, above), released with redactions; attached executed two-page contract modification, withheld in full.

Information Withheld/Exemption(s)

(b)(7)(E)

Information regarding a system used to identify, analyze, and investigate threats against Secret Service protectees, the identity of which would disclose details about protective intelligence techniques.

(b)(6), (b)(7)(C)

Names, e-mail address, and phone numbers of Secret Service personnel
Name, signature, and e-mail address of third party

Document 14, USSS-000109-110

Description

Two page proposal prepared by contractor, dated September 15, 2011, regarding proposed contract modifications, withheld in full.

Information Withheld/Exemption(s) claimed

(b)(7)(E)

The description of proposed modifications to a system utilized in identifying, analyzing, and investigating threats against Secret Service protectees, including data retention capabilities, the disclosure of which would reveal details about protective intelligence techniques.

(b)(6), (b)(7)(C)

Names of third parties

(b)(4)

Price analysis of proposed modifications.

Document 15, USSS-000111-112

Description

An October 2010 e-mail exchange between Agency personnel and contractor regarding initial implementation, released with redactions.

Information Withheld/Exemption(s)

(b)(7)(E)

Details regarding the implementation of a system utilized in identifying and investigating threats against Secret Service protectees, the disclosure of which would identify details about protective intelligence techniques.

Secret Service conference center access numbers and codes, the disclosure of which would allow unauthorized individuals to potentially gain access to sensitive

information

(b)(6), (b)(7)(C)

Names and phone number of Secret Service personnel
Names of third parties

Document 16, USSS-000113-125

An eight-page contract with a solicitation issue date of July 13, 2010, and a six-page statement of work (attached to January 12, 2011 e-mail in Document 15, above), withheld in full.

Information Withheld/Exemption(s)

(b)(4)

Confidential company pricing information

(b)(7)(E)

Information regarding a system used to identify, analyze and investigate potential threats against Secret Service protectees, including its functionality, the details of which would disclose information about protective intelligence techniques.

(b)(6), (b)(7)(C)

Names, phone numbers and e-mail addresses of Secret Service personnel

Document 17, USSS-000126-151

Description

Twenty-five page technical and management proposal plus one page cover letter submitted to the Secret Service by third party dated August 9, 2010, withheld in full.

Information Withheld/Exemption(s) claimed

(b)(7)(E)

Details, including functionality, regarding system utilized in identifying, analyzing, and investigating threats against Secret Service protectees, the identity of which would disclose details about protective intelligence techniques.

(b)(6), (b)(7)(C)

Name of Secret Service personnel
Name, address, phone numbers and e-mail addresses of third parties

(b)(4)

Proprietary and confidential company commercial and financial information

Document 18, USSS-000152-53

Description

October 21, 2011 e-mails reflecting communications between Protective Intelligence and Assessment Division personnel and contractor regarding implementation of September contract modification, released with redactions.

Information Withheld/Exemption(s)

(b)(7)(E)

Information regarding the implementation of a system utilized in identifying, analyzing, and investigating threats against Secret Service protectees, the identity of which would disclose details about protective intelligence techniques.

(b)(6), (b)(7)(C)

Name, e-mail address, and phone number of Secret Service personnel
Name, titles, phone numbers and e-mail address of a third party

Document 19, USSS-000154-158

Description

Five-page October 14, 2011 e-mail chain reflecting communications between Protective Intelligence and Assessment Division personnel and contractor regarding support provided for the Asia Pacific Economic Cooperation (APEC) , withheld in full.

Information Withheld/Exemption(s)

(b)(7)(E)

Information on a technique and on the procedures used in identifying potential threats against Secret Service protectees and conducting protective intelligence investigations.

(b)(6), (b)(7)(C)

E-mail address and phone number of Secret Service personnel
Names of Secret Service personnel
Name, e-mail address and phone number of a third party

Document 20, USSS-000159

Description

January 4, 2012 e-mail reflecting communications between Protective Intelligence and Assessment Division personnel and contractor, withheld in full.

Information Withheld/Exemption(s)

(b)(7)(E)

Information on a technique and on the procedures used in identifying potential threats against Secret Service protectees and conducting protective intelligence investigations.

(b)(6), (b)(7)(C)

Names of Secret Service personnel; phone number of Secret Service personnel
Name of a third party

Document 21, USSS-000160-179

Description

October 5, 2010 e-mail from contractor, released with redactions; attached nineteen page PowerPoint presentation regarding project kickoff, withheld in full.

Information Withheld/Exemption(s) claimed

(b)(6), (b)(7)(C)

Name of Secret Service personnel
Name, title, contact numbers, and e-mail addresses of third party

(b)(7)(E)

Details regarding system utilized in identifying, analyzing, and investigating threats against Secret Service protectees, including its functionality, the disclosure of which would reveal details about protective intelligence techniques.

Document 22, USSS-000180-192

Description

October 6, 2010 e-mail from contractor to Secret Service employee, released with redactions; attached questionnaire and information exchange documentation, withheld in full.

Information Withheld/Exemption(s) claimed

(b)(6), (b)(7)(C)

Name of Secret Service personnel
Name, title, contact numbers, and e-mail address of third party

(b)(7)(E)

Information and details about a technique and the procedures utilized in identifying, analyzing, and investigating threats against Secret Service protectees.

Information regarding a system used as part of the above referenced law enforcement technique, the identity of which would disclose details about the technique.

Document 23, USSS-00193-218

Description

October e-mail chain reflecting communications between Secret Service employees and contractor regarding program implementation, released with redactions; twenty-four pages of attached contractor access applications, withheld in full.

Information Withheld/Exemption(s) claimed

(b)(6), (b)(7)(C)

Names of Secret Service personnel
Names, addresses, contact numbers, e-mail addresses, social security numbers, drivers license numbers, and dates of birth of third parties

(b)(7)(E)

Details regarding a technique, including procedures and the name and configuration of a system used as part of the technique, utilized in identifying, analyzing, and investigating threats against Secret Service protectees.

Document 24, USSS-000219-220

Description

September 2010 e-mails between contractor and Secret Service employee requesting details in regard to a presentation at Secret Service Headquarters, released with redactions.

Information Withheld/Exemption(s) claimed

(b)(6), (b)(7)(C)

Name, e-mail and phone number of Secret Service personnel
Name, titles, contact numbers, and e-mail address of third party

Document 25, USSS-00221

Description

January 3, 2012 e-mails between contractor and Protective Intelligence and Assessment Division employees regarding contractors who have been granted building access, released with redactions.

Information Withheld/Exemption(s) claimed

(b)(6), (b)(7)(C)

Names and contact numbers of Secret Service personnel

Names and e-mail address of third party

Document 26, USSS-00222-223

Description

E-mails from third party to Secret Service employees, dated June 22, 2010, concerning request for proposal and bid process time frame, released with redactions.

Information Withheld/Exemption(s) claimed

(b)(6), (b)(7)(C)

Names, contact numbers and e-mail address of Secret Service personnel
Name, title, contact numbers and e-mail address of third party

(b)(7)(E)

Details regarding the requirements for a program used as part of a technique to identify, analyze, and investigate threats against Secret Service protectees.

Document 27, USSS-000224

Description

E-mail from contractor to Secret Service employee, dated October 19, 2010, regarding project logistics, released with redactions.

Information Withheld/Exemption(s) claimed

(b)(6), (b)(7)(C)

Name of Secret Service personnel
Name, title, contact numbers and e-mail address of third party

(b)(7)(E)

Details regarding the requirements for a program used to identify, analyze, and investigate threats against Secret Service protectees, used as part of a protective intelligence technique.

Document 28, USSS-000225-229

Description

2010 e-mail chain reflecting communications between third party and Secret Service employees regarding the procurement process, pricing, an outside training opportunity, and program capabilities, released with redactions.

Information Withheld/Exemption(s) claimed

(b)(4)

Proprietary information regarding company pricing structure

(b)(6), (b)(7)(C)

Names, contact numbers, and e-mail address of Secret Service personnel
Name, contact numbers and e-mail address of third party

(b)(7)(E)

Information on a system used to identify, analyze, and investigate threats against Secret Service protectees, the identity of which would disclose details about protective intelligence techniques.

Secret Service conference center access numbers and codes, the disclosure of which would allow unauthorized individuals to potentially gain access to sensitive information

Document 29, USSS-000230

Description

E-mails between contractor and Secret Service employee, dated September 29, 2010, requesting permission to use the Secret Service as a reference, released with redactions.

Information Withheld/Exemption(s) claimed

(b)(4)

Confidential commercial information

(b)(6), (b)(7)(C)

Names, contact numbers, and e-mail address of Secret Service personnel
Name, address, contact numbers and e-mail address of third party

Document 30, USSS 000231-232

Description

September 17, 2010 e-mail chain reflecting communications between third party and Secret Service employee regarding contract negotiations, released with redactions.

Information Withheld/Exemption(s) claimed

(b)(6), (b)(7)(C)

Names, contact numbers, and e-mail address of Secret Service personnel
Name, title, contact numbers and e-mail address of third party

(b)(7)(E)

Information about a system to be used to identify, analyze, and investigate threats against Secret Service protectees, the identity of which would disclose details about protective intelligence techniques.

Document 31, USSS 000233-234

Description

September 27, 2010 e-mails between contractor and Secret Service employee regarding project implementation, released with redactions.

Information Withheld/Exemption(s) claimed

(b)(6), (b)(7)(C)

Names, contact numbers, and e-mail address of Secret Service personnel
Name, title, contact numbers and e-mail addresses of third parties

Document 32, USSS 000235-241

Description

E-mail chain reflecting communications between third party and Secret Service employee regarding break down of pricing components and questions regarding the contracting process, released with redactions.

Information Withheld/Exemption(s) claimed

(b)(6), (b)(7)(C)

Names of Secret Service personnel
Name, title, contact numbers and e-mail address of third party

(b)(7)(E)

Details regarding configuration and capabilities of a system to be used to identify, analyze, and investigate threats against Secret Service protectees, the identity of which would disclose details about protective intelligence techniques.

(b)(4)

Proprietary and confidential company pricing information

Document 33, USSS 000242-243

Description

February 2010 e-mail chain involving third party and Secret Service employees reflecting a cost proposal, released with redactions.

Information Withheld/Exemption(s) claimed

(b)(6), (b)(7)(C)

Names of Secret Service personnel
Name, title, contact numbers and e-mail address of third party

(b)(7)(E)

Details regarding configuration and capabilities of a system to be used to identify,

analyze, and investigate threats against Secret Service protectees, the identity of which would disclose details about protective intelligence techniques.

(b)(4)

Proprietary and confidential company pricing information

Document 34 USSS 000244-267

Description

September 2011 e-mail chain between Protective Intelligence and Assessment Division employees and contractor regarding initial project implementation, released with redactions; attached twenty-one pages related to initial system configuration, withheld in full.

Information Withheld/Exemption(s) claimed

(b)(6), (b)(7)(C)

Names, contact numbers, and e-mail addresses of Secret Service personnel
Names, contact number, address, and e-mail address of third party

(b)(7)(E)

Details regarding a technique, including procedures and the configuration of a system used as part of the technique, utilized in identifying, analyzing, and investigating threats against Secret Service protectees.

Document 35, USSS-000268-269

Description

January 12, 2012 e-mail from third party to Secret Service employee providing pricing proposal and information regarding capabilities, released with redactions.

Information Withheld/Exemption(s)

(b)(4)

Proprietary company commercial and financial information

(b)(7)(E)

Information regarding a program to be utilized in identifying, analyzing, and investigating threats against Secret Service protectees, the identity of which would disclose details about protective intelligence techniques.

(b)(6), (b)(7)(C)

Name of Secret Service personnel
Name, title, contact number and e-mail address of a third party

Document 36, USSS-000270

Description

January 2007 e-mails from third party to Secret Service employee regarding anti-phishing services, released with redactions.

Information Withheld/Exemption(s)

(b)(6), (b)(7)(C)

Name and e-mail address of Secret Service personnel
Name, title, e-mail address, and contact numbers of a third party

Document 37, USSS-000271-273

Description

January 2010 e-mails reflecting communications between a Secret Service employee and a third party regarding an upcoming presentation, released with redactions.

Information Withheld/Exemption(s)

(b)(7)(E)

Information on a technique used in identifying potential threats against Secret Service protectees and conducting protective intelligence investigations.

(b)(6), (b)(7)(C)

Name and e-mail address of Secret Service personnel

Names, title, e-mail address, and contact numbers of third parties

Document 38, USSS-000274-275

Description

January 2010 e-mails between Secret Service employee and third party regarding an upcoming meeting, released with redactions.

Information Withheld/Exemption(s) claimed

(b)(6), (b)(7)(C)

Name and e-mail address of Secret Service personnel

Names, titles, contact number, and e-mail address of third parties

Document 39, USSS-000276-277

Description

January 5, 2010 e-mail from third party to Secret Service employee regarding vendor contacts, released with redactions.

Information Withheld/Exemption(s) claimed

(b)(6), (b)(7)(C)

Name of Secret Service personnel

Names, titles, contact numbers, and e-mail address of third parties

Document 40, USSS-00278-279

Description

January 6, 2010 e-mail from third party to Secret Service employee regarding meeting scheduling, released with redactions; attached biography of third party, withheld in full.

Information Withheld/Exemption(s) claimed

(b)(6), (b)(7)(C)

Name of Secret Service personnel

Name, title, e-mail address, and contact numbers of third party

Biography of third party

Document 41, USSS-000280-289

Description

June 2003 e-mails reflecting communication between Secret Service employees and third party, released with redactions; attached nine page white paper, released in full.

Information Withheld/Exemption(s) claimed

(b)(6), (b)(7)(C)

Names and e-mail addresses of Secret Service personnel
Names, title, contact number, and e-mail address of third parties

Document 42, USSS-00290-310

Description

November 2003 e-mails involving Secret Service personnel and third party reflecting the scheduling of a presentation, released with redactions; twenty pages of attachments, released in full.

Information Withheld/Exemption(s) claimed

(b)(6), (b)(7)(C)

Names and e-mail addresses of Secret Service personnel
Name, e-mail address, and contact numbers of third party