

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

_____)	
ELECTRONIC FRONTIER FOUNDATION)	
)	
Plaintiff,)	
)	Civil Action No. 1:06-cv-1708
v.)	
)	
DEPARTMENT OF JUSTICE,)	
)	
Defendant.)	
_____)	

EIGHTH DECLARATION OF DAVID M. HARDY

I, David M. Hardy, declare as follows:

(1) I am currently the Section Chief of the Record/Information Dissemination Section (“RIDS”), Records Management Division (“RMD”), formerly at Federal Bureau of Investigation Headquarters (“FBIHQ”) in Washington, D.C., and currently relocated to Winchester, Virginia. I have held this position since August 1, 2002. Prior to my joining the FBI, from May 1, 2001 to July 31, 2002, I was the Assistant Judge Advocate General of the Navy for Civil Law. In that capacity, I had direct oversight of Freedom of Information Act (“FOIA”) policy, procedures, appeals, and litigation for the Navy. From October 1, 1980 to April 30, 2001, I served as a Navy Judge Advocate at various commands and routinely worked with FOIA matters. I am also an attorney who has been licensed to practice law in the State of Texas since 1980.

(2) In my official capacity as Section Chief of RIDS, I supervise approximately 231 employees who staff a total of ten (10) units and two field operational service center units whose collective mission is to effectively plan, develop, direct, and manage responses to requests

for access to FBI records and information pursuant to the FOIA; Privacy Act; Executive Order 12958, as amended; Presidential, Attorney General, and FBI policies and procedures; judicial decisions; and Presidential and Congressional directives. The statements contained in this declaration are based upon my personal knowledge, upon information provided to me in my official capacity, and upon conclusions and determinations reached and made in accordance therewith. My responsibilities also include the review of FBI information for classification purposes as mandated by Executive Order (“E.O.”) 12958, as amended,¹ and the preparation of declarations in support of Exemption 1 claims under the FOIA.² I have been designated by the Attorney General of the United States as an original classification authority and a declassification authority pursuant to E.O. Order 12958, as amended, § 1.3 and 3.1.

(3) Due to the nature of my official duties, I am familiar with the procedures followed by the FBI in responding to requests for information from its files pursuant to the provisions of the FOIA, 5 U.S.C. § 552, and the Privacy Act of 1974, 5 U.S.C. § 552a. Specifically, I am aware of the FBI’s response to the FOIA requests of the plaintiff, the Electronic Frontier Foundation (“EFF”), for documents related to two electronic surveillance systems. More specifically, plaintiff’s August 11, 2006 FOIA request seeks access to records pertaining to the FBI’s System DCS-3000 and Red Hook and any reports made by the FBI to Congress on the FBI’s use of these technologies.

(4) The FBI conducted a wide-ranging search for FBIHQ records which could potentially contain responsive information. Approximately 20,000 pages of potentially

¹ 60 Fed. Reg. 19825 (1995), and 68 Fed. Reg. 15315 (2003).

² 5 U.S.C. § 552 (b)(1).

responsive records were located and forwarded to RIDS personnel. The majority of records reviewed consisted of technical information contained in emails, ECs, training and instruction manuals, memorandums, tables and charts, reports, briefings, internal configuration sketches, statements of need, upgrade plans, critical needs statements, spending plans, tests, requests, legal opinions and analysis documents, meeting notes, system description documents, justification documents, standard operating procedures, security plans, assessments, DCS-3000 printouts, transition plans and other informal documents. Upon review by RIDS personnel and upon further consultation with technical staff, a large portion of the documents supplied were determined to be outside the scope of the request. 10,314 pages underwent further review, and 2,394³ pages were further determined to be outside the scope of the request. Finally, the FBI has actually processed 7,920 responsive pages. Of this number 2,675 pages were withheld in their entirety (which includes 293 pages withheld as duplicates). The FBI released 5,245 pages of which 188 pages were released in full and 5,057 pages were released in part. On September 29, 2008, the parties submitted a Joint Status Report to this Court in which they agreed to select a representative sample of 800 pages from the 7,920 responsive pages processed by the FBI. This declaration provides the Court and plaintiff with an explanation for the justifications of the withholding of information from the 762⁴ sample pages chosen by the plaintiff in accordance with Vaughn v. Rosen, 484 F.2d 820 (D.C. Cir. 1973), pursuant to FOIA Exemptions 1, 2, 5, 6, 7(C)

³This page count includes corrections made during the litigation stage where it was found that 27 pages were incorrectly marked as duplicates during processing.

⁴It was later decided by the parties that Plaintiff would select the documents to be used as the representative sample in this case. Plaintiff selected 762 such pages for inclusion in the Vaughn index.

and 7(E), 5 U.S.C. §§ 552 (b)(1), (b)(2), (b)(5), (b)(6), (b)(7)(C) and (b)(7)(E).

CHRONOLOGY OF PLAINTIFF'S FOIA REQUEST

(5) By letter dated August 11, 2006 addressed to the FBI, Marcia Hoffman submitted a FOIA request on behalf of plaintiff, the Electronic Frontier Foundation (“EFF”), for “[a]ll records (including, but not limited to, electronic records) concerning electronic surveillance systems known as DCS-3000 and Red Hook, to include any reports made by the FBI to Congress on the Bureau’s use of these technologies.” In its letter, EFF also requested a waiver of all duplication and search/review fees associated with this FOIA request. **(See Exhibit A).**

(6) By two separate letters both dated August 22, 2006, FBIHQ acknowledged receipt of plaintiff’s FOIA request, and notified plaintiff that the request for DCS-3000 and Red Hook had been assigned FOIPA Request Nos. 1056287-000 and 1056307-000, respectively. **(See Exhibit B.)**

(7) By letter dated August 30, 2006, FBIHQ advised plaintiffs that a search of the automated indices to the FBI’s Central Records System (“CRS”) located no main Headquarters files responsive to its DCS-3000 request.⁵ Plaintiff was also advised that it could appeal the FBI’s determination to the U.S. Department of Justice, Office of Information and Privacy (“OIP”).⁶ **(See Exhibit C).**

⁵ FBIHQ conducted a similar search for plaintiff’s request for “Red Hook” documents, and that search located one responsive main Headquarters file. That file will be processed along with the other responsive records located as a result of the further search.

⁶ Documents responsive to plaintiff’s request were later located as a result of documents identified in response to an Electronic Communication (“EC”). This EC was addressed to all FBIHQ divisions believed most likely to possess records potentially responsive to plaintiff’s request, and directed each office to conduct a search of their records for that potentially responsive material.

(8) By letter dated January 9, 2007, FBIHQ provided plaintiff with documentation of a telephone conversation between a RIDS employee and plaintiff's counsel, Marcia Hofmann. This letter reiterated that:

(a) the records found to be responsive to plaintiff's requests totaled approximately 20,000 pages; and

(b) the FBI, in discussions with Ms. Hofmann, attempted to narrow the scope of the request in order to reduce the numbers of potentially-responsive records, thereby accelerating the processing, but these efforts were unsuccessful.

(See Exhibit D).

(9) In my Declaration dated February 9, 2007, (hereinafter the "First Hardy Declaration"), I advised the Court that the FBI had located approximately 20,000 pages potentially responsive to plaintiff's request and that plaintiff's request would be placed in the FOIA large queue of the "perfected" case backlog. Plaintiff's request came out of the FOIA large queue on May 9, 2007 and was assigned for processing on May 10, 2007.

(10) From June 4, 2007 through February 11, 2008, the FBI made interim releases of responsive records every four weeks pursuant to this Court's Order of May 5, 2007 until the entire production had been completed." Copies of the release letters may be found at **Exhibits E-N.**

**EXPLANATION OF CODED FORMAT USED FOR THE
JUSTIFICATION OF DELETED MATERIAL**

(11) All documents were processed to achieve maximum disclosure consistent with the access provisions of the FOIA. Every effort was made to provide plaintiff with all material in the public domain and with all reasonably segregable portions of releasable material. No reasonably

segregable, nonexempt portions were withheld from plaintiff. To further describe the information withheld could identify the very material which the FBI seeks to protect. Copies of the pages chosen by the plaintiff as a representative sample and released in part and in full are attached hereto as **Exhibit O**. A deleted page sheet has been inserted in place of pages withheld in their entireties. The previously released pages have been consecutively numbered DCS-3000-1 through DCS-3000-7888, and **Exhibit O** represents the documents chosen by the plaintiff as a representative sample. The total number of pages chosen by plaintiff for inclusion in this Vaughn index is 762 pages. The FBI asserts FOIA Exemptions (b)(1), (b)(2), (b)(5), (b)(6), (b)(7)(C), and (b)(7)(E) within the Vaughned pages as grounds for non-disclosure.

(12) Copies of the designated documents contain, on their face, coded categories of exemptions which detail the nature of the information withheld pursuant to the provisions of the FOIA. The coded categories are provided to aid the Court's and plaintiff's review of the FBI's explanations of FOIA exemptions used to withhold the protected material. A review of this information will reveal that all material withheld is exempt from disclosure pursuant to FOIA exemptions, or it is so intertwined with protected material that segregation is not possible without revealing the underlying protected material.

(13) Each withholding of information is accompanied by a code that corresponds to the categories listed below. For example, if "(b)(7)(C)-1" appears on the page, the "(b)(7)(C)" designation refers to "Exemption (b)(7)(C)" of the FOIA concerning "Unwarranted Invasion of Personal Privacy." The subcategory "1" narrows the main category into the more specific subcategory "Names and/or Identifying Information of FBI Support Personnel and Special Agents." The coded categories of exemptions used in the processing of documents responsive to

plaintiff's requests are set forth as follows:

SUMMARY OF JUSTIFICATION CATEGORIES	
CODED CATEGORIES	INFORMATION WITHHELD
Category (b)(1)	CLASSIFIED INFORMATION
(b)(1)	Information Properly Classified by an FBI Classification Authority Pursuant to Executive Order 12958, As Amended
Category (b)(2)	INTERNAL AGENCY RULES AND PRACTICES
(b)(2)-1	Information Related Solely to the Internal Practices and Procedures of the Agency and the Rules and Procedures Utilized for the Development and Operation of the DCS-3000 and Similar Systems (Cited in conjunction with (b)(7)(E)-1)
(b)(2)-2	Telephone and Facsimile Numbers, and Secure E-Mail and Web Site Addresses of FBI Personnel, Units, Design and Application Materials and Training Materials (Sometimes cited in conjunction with (b)(6)-1 and (b)(7)(C)-1)
Category (b)(5)	PRIVILEGED INFORMATION
(b)(5)-1	Deliberative Process Privilege
(b)(5)-2	Attorney-Client Privilege
Categories (b)(6) and (b)(7)(C)	CLEARLY UNWARRANTED AND UNWARRANTED INVASION OF PERSONAL PRIVACY
(b)(6)-1 and (b)(7)(C)-1	Names and/or Identifying Information of FBI Support Personnel and Special Agents (Sometimes cited in conjunction with (b)(2)-2.)
(b)(6)-2 and (b)(7)(C)-2	Names and/or Identifying Data of Third Parties of Investigative Interest
Category (b)(7)(E)	INVESTIGATIVE TECHNIQUES AND PROCEDURES
(b)(7)(E)-1	DCS-3000 and Similar Systems' Data Sources, Data Processes, Systems Design and Applications (Cited in conjunction with (b)(2)-1.)

JUSTIFICATION FOR REDACTIONS

(14) The paragraphs that follow explain the FBI's rationale for withholding each particular category of information under the specific exemption categories described above.

EXEMPTION (b)(1)
CLASSIFIED INFORMATION

(15) The FBI's analysis of the withholding of classified information contained in these documents is based on the standards articulated in the FOIA statute, 5 U.S.C. § 552 (b)(1).

Exemption (b)(1) protects from disclosure those records that are:

- (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and
- (B) are in fact properly classified pursuant to such Executive order.

(16) The FBI's analysis of whether Exemption (b)(1) permits the withholding of agency records consists of two significant steps. First, the FBI must determine whether the information contained in the records is information that satisfies both the substantive and procedural criteria of the applicable Executive Order governing the classification and protection of national security information. Second, the FBI has to analyze whether the documents are exempt pursuant to Exemption (b)(1). Thus, the first step is to examine whether the information satisfies the current Executive Order ("E.O.") 12958, as amended on March 25, 2003. E.O. 12958, as amended, governs the classification and protection of information that affects the national security,⁷ and prescribes various substantive and procedural criteria. I am bound by the requirements of E.O. 12958, as amended, when making classification determinations.

⁷ Section 6.1(y) of E.O. 12958, as amended, defines "National Security" as "the national defense or foreign relations of the United States."

(17) In order for information to be properly classified, and thus properly withheld from disclosure pursuant to Exemption (b)(1), the information must meet the requirements set forth in E.O. 12958, as amended, § 1.1 (a):

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

(18) As I will explain in further detail below, in my role as an original classification authority, I have determined that the information withheld pursuant to Exemption (b)(1) is under the control of the United States Government, is classified and requires a classification marking at the “Secret” level since the unauthorized disclosure of this information reasonably could be expected to cause serious damage to national security. See E.O. 12958, as amended, § 1.2(a)(2). In addition to these substantive requirements, certain procedural and administrative requirements of E.O. 12958, as amended, must be followed before information can be considered to be properly classified, such as, proper identification and marking of documents. In particular, I made certain that all procedural requirements of E.O. 12958, as amended, were followed, and made certain that:

- (1) the document was marked as required and stamped with the proper

classification designation;⁸

- (2) the document was marked to indicate clearly which portions are classified, which portions are exempt from declassification as set forth in E.O. 12958, as amended, § 1.5 (b), and which portions are unclassified;⁹
- (3) the prohibitions and limitations on classification specified in E.O. 12958, as amended, § 1.7, were adhered to;
- (4) the declassification policies set forth in E.O. 12958, as amended, § 3.1 were followed; and
- (5) any reasonably segregable portions of the classified document that did not meet the standards for classification under E.O. 12958, as amended, were declassified and marked for release, unless withholding was otherwise warranted under applicable law.

FINDINGS OF DECLARANT REGARDING EXEMPTION (b)(1)

(19) With the above requirements in mind, I personally and independently examined the FBI information withheld pursuant to FOIA Exemption (b)(1). Classified information has been withheld on the following pages: DCS-3000-1542, 2847, 3443, 3460, 5280, 5282-5283, 5285-5286, 5489, 7525, 7711-7716, 7726, 7728-7733, 7779-7801, 7867-7868, 7882-7883, 7885, 7887. I determined that this classified information continues to warrant classification at the “Secret” level, and is exempt from disclosure pursuant to E.O. 12958, as amended, § 1.4, categories (c) intelligence activities, (d) foreign relations or foreign activities of the U.S., and (g) vulnerabilities and capabilities of systems, as the unauthorized disclosure of the information could reasonably be expected to cause serious damage to the national security.

⁸ E.O. 12958, as amended, §§ 1.6 (a)(1)-(5).

⁹ E.O. 12958, as amended, § 1.6 (c).

INTELLIGENCE ACTIVITIES, SOURCES AND METHODS

(20) The classified information withheld on DCS-3000-1542, 2847, 3443, 3460, 5280, 5282-5286, 5489, 7525, 7711, 7712, 7714-7716, 7726, 7728, 7729, 7730-7733, 7779-7781, 7867, 7868, 7882, 7883, 7885 and 7887 identifies the names and/or provides identifying descriptions of systems that are intelligence methods used as an effective means for the FBI to gather, store or disseminate intelligence information. The classified information obtained from this system is very specific in nature and known to very few individuals. The release of this information would obviate the effectiveness of these intelligence gathering methods. The identification of these intelligence methods, which continue to furnish positive intelligence information to date, will severely limit their application. In addition, disclosure will inform hostile intelligence of the possible range of our intelligence capabilities, as well as the probable intelligence that the FBI has gathered, or can collect, concerning them. This knowledge provides potential or actual violators of the national security laws of the United States a means of deflection or avoidance of lawful laws, policies, and regulations. Disclosure will allow countermeasures to be implemented, making future operations more difficult, or compromise other ongoing planned intelligence operations. Accordingly, the release of the names of these classified systems and/or their descriptive data can lead to the exposure of the actual intelligence activities or methods utilized in FBI investigations, and can reasonably be expected to cause serious damage to national security. The names of these systems and any identifying descriptive data are properly classified at the "Secret" level and withheld pursuant to E.O. 12958, as amended, § 1.4 (c) and are exempt from disclosure pursuant to Exemption (b)(1).

FOREIGN RELATIONS

(21) Section 1.4 (d) of E.O. 12958, as amended, protects information from disclosure if its release would reveal foreign relations or foreign activities of the United States, including confidential sources. The systems and descriptive data identified on DCS-3000-1542 contain sensitive information gathered by the United States either about or from a foreign country. Information that affects the foreign relations of the United States, much like foreign government information, does not lose its sensitivity with the passage of time. The delicate liaison established between the United States and these foreign governments could be severely damaged should the United States disclose these investigations. As a result, this information must be handled with care so as not to jeopardize the fragile relationships that exist among the United States and certain foreign governments. The unauthorized disclosure of this information concerning foreign relations or foreign activities of the United States can reasonably be expected to lead to diplomatic or economic retaliation against the United States; identify the target, scope or time frame of intelligence activities of the United States in or about a foreign country, which may result in the curtailment or cessation of these activities; enable hostile entities to assess United States intelligence-gathering activities in or about a foreign country and devise countermeasures against these activities; or compromise cooperative foreign sources which may jeopardize their safety and curtail the flow of information from these sources. As a result, I have determined that this information is properly classified at the "Secret" level, properly withheld pursuant to E.O. 12958, as amended, § 1.4 (d), and exempt from disclosure pursuant to FOIA Exemption (b)(1).

VULNERABILITIES OR CAPABILITIES OF SYSTEMS

(22) Classified information has been withheld on DSC-3000-1542, 2847, 3460, 5280, 5282, 5283, 5285, 5286, 5289, 7525, 7711, 7712, 7714-7716, 7726, 7728 and 7731-7733 under Section 1.4 (d) of E.O. 12958, as amended in order to protect the vulnerabilities and/or capabilities of the DCS-3000 and similar systems from disclosure. If such information were disclosed, the FBI would be providing a roadmap on how to evade the detection of illegal activity of an actual or potential criminal or terrorist. If this information were made public, an individual would then know what the capabilities and weaknesses of the DCS-3000 and similar systems are and therefore know not only how to avoid detection but would know where and how to attack these systems. Many of the capabilities and vulnerabilities of the DCS-3000 and similar systems are discussed in emails of FBI employees, documented in charts, graphs, and discussed in depth in the various training manuals and similar documents contained in the release. If the totality of this information is released, it would allow individuals to adapt their activities and methods in order to avoid future detection. Additionally, the release of data processes, systems design and applications could result in vulnerabilities to potential security attacks and invasions. Accordingly, the FBI properly withheld this information pursuant to FOIA Exemption (b)(1).

**DEFENDANT'S BURDEN OF ESTABLISHING
EXEMPTION (b)(1) CLAIMS**

(23) In this instance I have determined that the disclosure of this information could reasonably be expected to cause serious damage to the national security, and its withholding outweighed the benefit of disclosure. In reaching this conclusion, I exercised my prerogative as an original classification authority and designated the information as classified in the interest of national security, and invoked Exemption (b)(1) of the FOIA to prevent disclosure. The

justifications for the withheld information should be read in the context in which the classified information is found. This context includes not only the surrounding unclassified information on the remainder of the page, but also other information which already exists in the public domain, as well as information likely known or suspected by hostile intelligence entities. It is my judgment that any greater specificity in the descriptions and justifications set forth with respect to the names and descriptive data of the systems at issue, disclosure of which would reveal intelligence activities and foreign relations or foreign activities of the U.S., impact foreign relations, and reveal the capabilities and vulnerabilities of systems, could reasonably be expected to jeopardize the national security of the United States.

EXEMPTION (b)(2)
INTERNAL AGENCY RULES AND PRACTICES

(24) 5 U.S.C. § 552 (b)(2) exempts from disclosure information “related solely to the internal personnel rules and practices of an agency.”

(25) This exemption encompasses two distinct categories of records that are internal in nature: those involving trivial administrative matters of no genuine public interest (“Low” 2), and those the disclosure of which would risk circumvention of a statute or regulation (“High” 2).

(b)(2)-1 **Information Related Solely to the Internal Practices and Procedures of the Agency and the Rules and Procedures Utilized for the Development and Operation of the DCS-3000 and Similar or Related Systems (Cited in conjunction with (b)(7)(E)-1)**

(26) Exemption (b)(2)-1 (High) has been asserted in conjunction with Exemption (b)(7)(E)-1 to protect information related solely to the internal practices and procedures of the agency and the rules and procedures utilized for the development and operation of the DCS-3000 and similar or related systems. Development of the DCS-3000 and similar systems has become

necessary due to the fact that certain new and emerging technologies are not covered by the Communications Assistance for Law Enforcement Act (“CALEA”). The DCS-3000 is an interim solution, developed by the FBI, to intercept personal communications services delivered via emerging digital technologies used by wireless carriers in advance of any CALEA solutions being deployed. Red Hook is another system developed by the FBI to collect voice and data calls and then process and display the intercepted information in the absence of a CALEA solution.

(27) The FBI’s priorities shifted dramatically away from its traditional law enforcement mission after the September 11, 2001 terrorist attacks. Our top three priorities are now counterterrorism, counterintelligence, and cyber security. The DCS-3000 and similar systems are digital collection tools used to facilitate the collection of communications which are then used in furtherance of the FBI’s counterterrorism, counterintelligence and investigative efforts. Traditional telephones were the primary avenue criminals used to communicate information regarding unlawful acts in the past. Today, more and more incidents are committed and facilitated by terrorists and other criminals using high-tech, non traditional communication methods. The FBI must develop and utilize constantly evolving tools and technology in order to perform its mission.

(28) The types of documents for which the exemption is claimed can be categorized as follows: (1) policy, planning, and operations documents; (2) FBI internal e-mails; (3) FBI “Electronic Communications” (“ECs”); and (4) other miscellaneous documents. The exemption is applied to information considered to be either: (1) a data source, (2) a data process, (3) a computer application, or (4) a systems design.

(29) The majority of information withheld pursuant to Exemption (b)(2)-1 is contained

in DCS-3000 policy, planning, and operations documents. These documents contain details about DCS-3000 system design, including access to data, data attributes, and administrative procedures, development, capabilities and vulnerabilities of the system, and training materials and manuals for operation of the DCS-3000.

(30) The second category of documents to which the (b)(2)-1 exemption is applied are FBI internal e-mails. Subjects of the e-mails include, but are not limited to, discussion of proposed and existing sources of information, methods of gathering information, draft Privacy Threshold Analysis, and DCS-3000 design, processes and applications.

(31) Other miscellaneous documents in which the (b)(2)-1 exemption is asserted are printouts from the DCS-3000, legal opinions and analysis, Transition Plans, and an article.

(32) The release of DCS-3000 data sources, data processes, systems design and applications, would risk circumvention of the law by those organizations or individuals who seek to undermine or destroy the integrity of the DCS-3000. Specifically, by disclosing the data sources and types of sources of information available to and utilized by the DCS-3000, the FBI would be providing a roadmap on how to evade the detection of illegal activity of an actual or potential criminal or terrorist. If these sources were made public, an individual would then know from where the DCS-3000 obtains its information and he or she could avoid utilizing these methods of communication. If the methods of obtaining the communications, the types of communications which are obtained, and the sources from which these communications are obtained were revealed, it would allow individuals to adapt their activities and methods in order to avoid detection. Additionally, the release of data processes, systems design and applications could result in vulnerabilities to potential cyber attacks and invasions. Accordingly, the FBI

properly withheld this information pursuant to FOIA Exemption (b)(2)-1 on the following pages: DCS-3000-3-6, 11, 232, 964, 966, 1198, 1252, 1386, 1417, 1455, 1459-1460, 1542, 1605-1609, 1667, 1713, 1761, 1882-1884, 1957, 2034, 2074-2078, 2207, 2846-2847, 3131-3132, 3138, 3443, 3452-3453, 3459-3460, 3494-3495, 3520-3524, 3569-3570, 3572-3573, 3582, 3584, 3586, 3599-3603, 3605-3612, 3614, 3621-3628, 3632-3633, 3639, 3641-3642, 3683-3696, 3749-3752, 3758-3761, 3769-3776, 3805-3826, 3841-3869, 3929-3942, 3987-4011, 4087- 4122, 4193-4230, 4232, 4235-4236, 4241-4255, 4257-4258, 4261-4265, 4268-4271, 4274- 4275, 4277-4279, 4281, 4344- 4349, 4730-4735, 4975-4977, 5061, 5063-5064, 5069-5079, 5087-5094, 5104, 5106 -5109, 5112-5113, 5116-5131, 5135-5142, 5144-5148, 5153-5154, 5156-5201, 5203, 5208, 5210-5212, 5214, 5220-5231, 5233-5239, 5242, 5244-5254, 5256, 5259-5267, 5269, 5272-5276, 5278, 5280-5286, 5489-5495, 5497-5503, 5522, 7524-7525, 7527-7533, 7535-7540, 7542-7544, 7546-7549, 7551-7553, 7555, 7711-7716, 7721-7733, 7779-7801, 7809-7817, 7821-7824, 7840, 7847 and 7859-7888.

(b)(2)-2 Telephone and Facsimile Numbers, Secure E-Mail and Web Site Addresses of FBI Personnel & System Applications

(33) Exemption (b)(2)-2 (Low) has been asserted (sometimes in conjunction with (b)(6)-1 and (b)(7)(C)-1) to protect internal telephone and facsimile numbers, e-mail addresses, and web site addresses of FBI personnel as well as the internal web pages utilized by the various FBI Units for transfer of information concerning the systems design, processes, and applications related to DCS-3000 including, but not limited to, training materials for the DCS-3000.

Telephone and fax numbers and e-mail and web site addresses clearly relate to the internal practices of the FBI in that they are utilized by FBI personnel during the performance of their jobs. Disclosure of these types of contact information could subject these individuals to

harassing telephone calls or e-mails which could disrupt official business (including by impeding the ability of Special Agents to conduct and conclude law enforcement investigations in a timely manner). Release of the internal web addresses of manuals and training materials for the DCS-3000 serves no public benefit since these are internal web locations not accessible by the public. Routine internal administrative information such as the numbers, addresses and webpages referenced above serve no public benefit, and there is no indication that there is a genuine public interest in the disclosure of this information. Accordingly, because these internal phone numbers and computer addresses are related to the FBI's internal practices, because disclosure would not serve any public interest, and because disclosure could impede the FBI's effectiveness, the FBI withheld this information pursuant to Exemption (b)(2)-2 on the following pages: DCS-3000-5, 232, 1403a, 1455, 1459, 1609, 2033, 2074-2075, 2077 -2078, 3132, 3443, 3452, 3496, 3519, 3573, 3582, 3584, 3586, 5060, 5080, 5094, 5117, 5142, 5154-5155, 5213, 5219, 5277, 5490, 7809-7817, 7821-7824, 7840, 7847, 7859-7867, 7869-7887.

EXEMPTION (b)(5)
PRIVILEGED INFORMATION

(34) 5 U.S.C § 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 exempt those documents or information normally privileged in the civil discovery context, and it includes the deliberative process and attorney-client privileges, both of which are claimed in this release.

(b)(5)-1 **Deliberative Process Privilege**

(35) The deliberative process privilege protects the internal deliberations of the

government by exempting from release recommendations, analyses, speculation and other non-factual information prepared in anticipation of agency decision-making. The general purpose of the deliberative process privilege is to prevent injury to the quality of agency decisions. Thus, material that contains or was prepared in connection with the formulation of opinions, advice, evaluations, deliberations, policy formulation, proposals, conclusions or recommendations may properly be withheld. Release of this type of information would have an inhibitive effect upon the development of policy and administrative direction of an agency because it would chill the full and frank discussion between agency personnel regarding a decision. If agency personnel knew that their preliminary opinions, evaluations and comments would be released for public consumption, they may be more circumspect in what they put in writing, and thereby, impede a candid discussion of the issues surrounding a decision.

(36) To invoke the deliberative process privilege, an agency must show that an allegedly exempt document is both (a) “predecisional” – antecedent to the adoption of agency policy; and agency must also pinpoint agency decision or policy to which document contributed . . . or . . . identify a decision making process to which a document contributed – and (b) “deliberative” – a direct part of the deliberative process in that it makes recommendations or express opinions on legal or policy matters, reflects the give and take of the consultative process, and bears on the formulation or exercise of agency policy-oriented judgment. Furthermore, an agency must identify the role of a contested document in a specific deliberative process.

(37) Accordingly, because the cited materials were prepared in the context of agency employees’ deliberations, because they consist of preliminary opinions, evaluations and comments of FBI staff, and because release of these exempted materials would chill the full and

frank discussion between agency personnel regarding agency decisions, the FBI has properly withheld this information pursuant to FOIA Exemption (b)(5)-1 either in part or in full the following pages of Exhibit O: DCS-3000-1606 through 1607, 1609, 2889 through 2895, 3494 through 3497, 3523 through 3524, 3543 through 3545, 3569, 3572 through 3573, 5289, 5493 through 5501.

(b)(5)-2 Attorney-Client Privilege

(38) Additionally, Exemption (b)(5) has been asserted to protect material covered by the attorney-client privilege. The attorney-client privilege is appropriately asserted when legal advice of any kind is sought from a professional legal adviser in his or her capacity as such and the communications relating to that purpose are made in confidence by the client. The communications are permanently protected from disclosure by the client or by the legal adviser unless the attorney-client protection is waived. This privilege encompasses confidential communications made to the attorney not only by decision-making personnel but also by lower-echelon employees who possess information relevant to an attorney's advice-rendering function. Disclosure of the two-way communications between FBI attorneys and their clients would impede the full disclosure of all of the information that relates to the client's reasons for seeking legal advice, which is necessary if the professional mission is to be accomplished.

(39) Exemption (b)(5)-2 has been applied to the following pages: DCS-3000-2889 through 2895, 3523, 3543 through 3545, 3569, 3573, and can be divided into two functional categories of documents: (1) FBI internal e-mails and (2) a Privacy Threshold Analysis. The majority of material withheld pursuant to Exemption (b)(5)-2 is contained in internal FBI e-mails.

(40) Most of the e-mails to which the (b)(5)-2 Exemption is applied were produced from the computers of the Office of General Counsel (“OGC”) employees. In every instance where the attorney-client privilege has been claimed in an e-mail, legal advice pertaining to some aspect of the DCS-3000 is provided by or sought from OGC attorneys.

(41) The attorney-client privilege has been invoked on a draft version of a Privacy Threshold Analysis. The Privacy Threshold Analysis was prepared for and contains responses intended for review by OGC. This document merits protection under the attorney-client privilege because it evidences OGC legal advice sought and provided.

(42) The FBI e-mails and the draft Privacy Threshold Analysis discussed above contain information being presented to OGC attorneys for consultation or OGC attorneys’ opinions on legal issues presented by the creation and utilization of the DCS-3000, all discussed within an internal FBI e-mail system. The attorney-client privilege has not been waived, and as a result, the FBI properly withheld this information pursuant to (b)(5)-2.

EXEMPTION (b)(6) AND (b)(7)(C)
CLEARLY UNWARRANTED AND UNWARRANTED
INVASION OF PERSONAL PRIVACY

(43) 5 U.S.C. § 552(b)(6) exempts from disclosure “personnel and medical files and similar files when the disclosure of such information would constitute a clearly unwarranted invasion of personal privacy. Moreover, 5 U.S.C. § 552 (b)(7)(C) exempts from disclosure:

records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . could reasonably be expected to constitute an unwarranted invasion of personal

privacy.¹⁰

EXEMPTION (b)(7) THRESHOLD

(44) Exemption (b)(7) of the FOIA protects from mandatory disclosure records or information compiled for law enforcement purposes, but only to the extent that disclosure could reasonably be expected to cause one of the harms enumerated in the subparts of the exemption. See 5 U.S.C. § 552(b)(7). In this case, the harm that could reasonably be expected to result from disclosure concerns the invasion of personal privacy and revealing sensitive law enforcement techniques.

(45) Before an agency can invoke any of the harms enumerated in Exemption (b)(7), it must first demonstrate that the records or information at issue were compiled for law enforcement purposes. Law enforcement agencies such as the FBI must demonstrate that the records at issue are related to the enforcement of federal laws and that the enforcement activity is within the law enforcement duty of that agency. The records responsive to plaintiff's request concern the creation and implementation of system designed to provide specific investigative data. The DCS-3000 is an essential investigatory tool used by FBI personnel. Thus, there is no doubt that this system and the information it gathers falls within the law enforcement duties of the FBI. Accordingly, the information readily meets the threshold requirement of Exemption (b)(7). The remaining inquiry is whether its disclosure "could reasonably be expected to

¹⁰ The practice of the FBI is to assert Exemption (b)(6) in conjunction with (b)(7)(C). Although the balancing test for (b)(6) uses a "would constitute a clearly unwarranted invasion of personal privacy" and the test for (b)(7)(C) uses the lower standard of "could reasonably be expected to constitute an unwarranted invasion of personal privacy," the analysis and balancing required by both exemptions is sufficiently similar to warrant a consolidated discussion. The privacy interests are balanced against the public's interest in disclosure under the analysis of both exemptions.

constitute an unwarranted invasion of personal privacy,” or “could reasonably be expected to risk circumvention of the law.”

(46) When withholding information pursuant to Exemptions (b)(6) and (b)(7)(C), the FBI is required to balance the privacy interests of the individuals mentioned in the documents against any public interest in disclosure. In asserting these exemptions, each piece of information was scrutinized to determine the nature and strength of the privacy interest of any individual whose name and/or identifying information appeared in the documents at issue. In making this analysis, the public interest was determined to be information which would shed light on the FBI’s performance of its mission to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners. In this case, the FBI concluded that the information should be withheld under Exemptions (b)(6) and (b)(7)(C), and determined that the individuals’ privacy interests were not outweighed by any public interest in disclosure.

**(b)(6)-1 and (b)(7)(C)-1: Names and/or Identifying Information
of FBI Support Personnel and Special Agents**

(47) Exemptions (b)(6)-1 and (b)(7)(C)-1 have been asserted, at times in conjunction with (b)(2)-2, to protect the names and identifying information (such as telephone numbers, telephone extensions, and facsimile numbers) of FBI support personnel and Special Agents. The privacy consideration applies to FBI support personnel and Special Agents, as individuals, from unnecessary, unofficial questioning as to their participation in the design, maintenance and use of FBI computer systems and databases which contain information about current and past investigations. FBI Special Agents were involved in the design of the DCS-3000. Their names

appear in e-mails contained in this release. In general, FBI Special Agents conduct official inquiries into various criminal and national security violation cases, and the DCS-3000 is one investigatory tool utilized. There is no public interest to be served by disclosing the identities of the Special Agents to the public. Thus, disclosure of this information would constitute a clearly unwarranted and unwarranted invasion of their personal privacy.

(48) The privacy consideration extends to support employees whose names appear in these files, including staff from the Operational Technology Division (“OTD”), various field offices, and the OGC. These employees have access to information regarding computer systems designs and security, and could become targets of harassing inquiries for unauthorized access to these systems if their identities were released. These individuals maintain substantial privacy interests in not having their identities disclosed. There is no public interest to be served by releasing the identities of these individuals. Thus, disclosure of this information would constitute a clearly unwarranted and unwarranted invasion of their personal privacy. Accordingly, the FBI properly protected this information pursuant to FOIA Exemptions (b)(6)-1 and (b)(7)(C)-1.

FOIA Exemptions (b)(6)-1 and (b)(7)(C)-1 has been cited on the following pages: DCS-3000-3-6, 11, 232, 1252, 1386, 1403a, 1403f, 1417, 1455, 1459-1460, 1542, 1605-1609, 1667, 1713, 1761, 1882-1884, 1957, 2033, 2074-2078, 2207, 2847, 2889, 2894-2895, 3131-3132, 3138, 3443, 3459-3460, 3494-3495, 3519-3520, 3523-3524, 3543-3545, 3569-3570, 3572, 4231, 4237, 4239, 4252, 4256, 4259, 4266, 4273, 4280, 4344, 5060-5062, 5064, 5067-5068, 5080, 5082, 5084-5086, 5094, 5103, 5114, 5117, 5133, 5142-5143, 5154-5156, 5207, 5209-5211, 5213-5216, 5238, 5277, 5279, 5289, 5490-5493, 5496, 5502-5503, 5522, 7524-7525, 7711-7712, 7714-7716, 7727-7728, 7780, 7792, 7794, 7809-7811 .

**(b)(6)-2 and (b)(7)(C)-2: Names and/or Identifying Information
of Third Parties of Investigative Interest**

(49) Exemptions (b)(6)-2 and (b)(7)(C)-2 have been asserted to protect the names and identifying information of third-party individuals who are of investigative interest to the FBI and/or other law enforcement agencies. Identifying information withheld concerning these third parties includes communications data and information that could potentially lead to the identification of the third party. Being linked with any law enforcement investigation carries a strong negative connotation and a stigma. Release of the identities of these individuals to the public could subject them to harassment or embarrassment, as well as undue public attention. Accordingly, the FBI has determined that these individuals maintain a substantial privacy interest in not having their identities disclosed. In making a determination whether to release the names and personal information concerning these third parties, the public's interest in disclosure was balanced against the individual's right to privacy. RIDS determined that this information would not enlighten the public on how the FBI conducts its internal operations and investigations. Accordingly, the FBI concluded that the disclosure of this information would constitute a clearly unwarranted and unwarranted invasion of their personal privacy and properly withheld this information pursuant to Exemptions (b)(6)-2 and (b)(7)(C)-2 on the following pages: DCS-3000-2074-2075, 2077-2078, 3808, 3811, 3814, 3822-3823, 3825, 3845-3846, 3854-3855, 3864, 3867, 4108-4109, 4195, 4197, 4198-4230, 4243, 4245, 4247-4251, 4261-4262, 4264, 4268-4269, 4271, 7528-7533, 7535-7540, 7868.

**EXEMPTION (b)(7)(E)
INVESTIGATIVE TECHNIQUES AND PROCEDURES**

(50) 5 U.S.C. § 552 (b)(7)(E) provides for the withholding of:

law enforcement records 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.

(b)(7)(E)-1 DCS-3000 Data Sources, Data Processes, Systems Design and Applications (Cited in conjunction with (b)(2)-1)

(51) Exemption (b)(7)(E)-1 has been asserted in conjunction with (b)(2)-1 to protect DCS-3000 data sources and processes, systems design and applications. The types of documents in which the exemption is claimed can be categorized as follows: (1) policy, planning, and operations documents; (2) FBI internal e-mails; (3) other miscellaneous documents. The exemption is applied to information considered to be: (1) a data source, (2) a data process, (3) a computer application, or (4) a systems design.

(52) More specifically, Exemption (b)(7)(E)-1 has been applied to internal database identifiers; data source information; computer systems and subsystems identification and descriptions of capabilities, including details about the storage, searching and management and control of data; external computer interfaces; detailed descriptions of types of data obtained through use of the DCS-3000 and similar systems; and similar or related system names and components. The (b)(7)(E)-1 Exemption has been cited in conjunction with Exemption (b)(2)-1. The (b)(7)(E)-1 Exemption has been applied to the same documents to which the (b)(2)-1 Exemption was applied.

(53) Exemption (b)(7)(E) applies to procedures which are unique in nature and not ordinarily known to the public. Although the DCS-3000's existence is known to the public, the specific design of the system, including DCS-3000 capabilities and vulnerabilities, data sources, and data transfer mechanisms, are not ordinarily known to the public. DCS-3000 training

materials, procedure manuals, security plans, transition plans, Privacy Threshold Analysis, development materials, charts, tables and other documents created for discussion of the capabilities and vulnerabilities of the DCS-3000 system are examples of documents identified in this release for which portions have been exempted under Exemption (b)(7)(E).

(54) The release of the details of any of these internal procedural documents could enable criminals to employ countermeasures to undermine the effectiveness of the DCS-3000 and thus jeopardize the FBI's investigatory missions. Classified data could be released, destroyed or manipulated if these procedures were made available to the public. The release of DCS-3000 data sources, data processes, systems design and applications would risk circumvention of the law by those organizations or individuals who seek to undermine or destroy the integrity of the DCS-3000. Specifically, by disclosing the capabilities and vulnerabilities of the DCS-3000, the FBI would be providing a roadmap on how to evade the detection of illegal activity of an actual or potential criminal or terrorist. If these sources were made public, an individual would then know how and from where the DCS-3000 obtains its information and he or she could avoid utilizing these methods of communication. If the totality of these sources were released, it would allow individuals to adapt their activities and methods in order to avoid future detection. Consequently, because the DCS-3000 is utilized for law enforcement investigations, because the DCS-3000 contains procedures utilized in law enforcement investigations and because disclosure of these procedures could reasonably be expected to risk circumvention of the law, the FBI properly withheld this information pursuant to Exemption (b)(7)(E)-1 on the following pages: DCS-3000-3-6, 11, 232, 964, 966, 1198, 1252, 1386, 1417, 1455, 1459-1460, 1542, 1605-1609, 1667, 1713, 1761, 1882-

1884, 1957, 2034, 2074-2078, 2207, 2846, 2847, 3131-3132, 3138, 3443, 3452-3453, 3459-3460, 3494-3496, 3520-3524, 3569-3570, 3572-3573, 3582, 3584, 3586, 3599-3603, 3605-3612, 3614, 3621-3627, 3628, 3632-3633, 3639, 3641-3642, 3683-3696, 3749-3752, 3758-3761, 3769-3776, 3805-3826, 3841-3869, 3929-3942, 3987-4011, 4087-4122, 4193-4228, 4232, 4241-4245, 4247-4252, 4254-4255, 4257-4258, 4261-4265, 4268-4271, 4274-4275, 4277-4279, 4281, 4344-4349, 4730-4735, 4975-4977, 5061, 5063, 5069-5079, 5087-5094, 5104, 5106-5109, 5112-5113, 5116-5131, 5135-5142, 5144-5148, 5153-5154, 5157-5201, 5203, 5208, 5210-5212, 5214, 5219-5231, 5233-5239, 5242, 5244-5254, 5256, 5259-5267, 5269, 5272-5276, 5278, 5280-5286, 5489, 5489-5495, 5497-5503, 5522, 7524, 7525, 7527-7533, 7535-7540, 7542-7544, 7546-7549, 7551-7553, 7555, 7711-7716, 7721-7733, 7779-7801, 7809-7817, 7821-7824, 7840, 7847, 7859-7861, 7863-7868, 7871-7873, 7875-7879, 7881-7888.

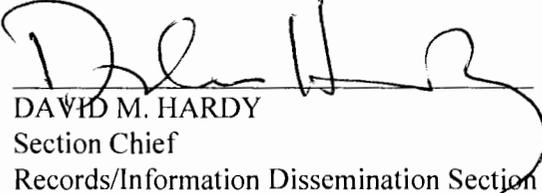
CONCLUSION

(55) The FBI has processed and released all reasonably segregable information from the records responsive to plaintiff's request to the FBI. The remaining information has been withheld pursuant to FOIA Exemptions 1, 2, 4, 5, 6, 7(A), 7(C), 7(D) and 7(E), 5 U.S.C. §§ 552 (b)(1), (b)(2), (b)(4), (b)(5), (b)(6), (b)(7)(A), (b)(7)(C), (b)(7)(D) and (b)(7)(E). The FBI has carefully examined the responsive documents and has determined that the information withheld from plaintiff, if disclosed, could reasonably be expected to cause serious damage to national security; could reasonably be expected to reveal internal administrative information; could divulge confidential commercial

information; could reveal privileged information; could cause unwarranted and clearly unwarranted invasion of the personal privacy interest of third parties; could interfere with law enforcement proceedings; and could disclose techniques and procedures for law enforcement investigations. Accordingly, the FBI has released all reasonably segregable, nonexempt information to plaintiff in response to its FOIA requests to the FBI.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct, and that Exhibits A through O attached hereto are true and correct copies.

Executed this 31st day of July, 2009.



DAVID M. HARDY
Section Chief
Records/Information Dissemination Section
Records Management Division
Federal Bureau of Investigation
Winchester, Virginia