IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

KEVIN POULSEN,

Plaintiff,

v.

U.S. CUSTOMS AND BORDER PROTECTION,

Defendant.
_____/

No. C 06-1743 SI

ORDER RE: CROSS-MOTIONS FOR SUMMARY JUDGMENT

On May 26, 2006, the Court heard oral argument on the parties' cross-motions for summary judgment. After the hearing, the Court ordered defendant to submit the documents at issue for *in camera* review. Defendant lodged those documents on June 6, 2006, and the Court has conducted its review. After careful consideration of the parties' papers and arguments, the Court concludes that some of the withheld information should be produced, and accordingly GRANTS in part and DENIES in part the cross-motions for summary judgment.

BACKGROUND

On March 7, 2006, plaintiff Kevin Poulsen, a journalist, filed this complaint under the Freedom of Information Act ("FOIA") seeking to compel defendant United States Customs and Border Protection ("CBP") to immediately process and disclose records and information responsive to an August 22, 2005, FOIA request. Plaintiff's FOIA request concerns an incident that occurred on August 18, 2005, when government computers that process incoming visitors to the United States unexpectedly shut-down, causing back-ups and delays. On August 19, 2005, the Associated Press reported that a Homeland

Security spokesman attributed the failure to a virus that impacted computer systems at a number of airports, including those in New York, San Francisco, Miami, Los Angeles, Houston, Dallas and Laredo, Texas. *See* Complaint, Ex. A.

Plaintiff submitted his initial request for documents under the FOIA by letter dated August 22, 2005. That letter sought the following:

> Any documents (including but not limited to electronic records) detailing, describing or concerning the August 18th, 2005 failure of a CBP computer system used to process passengers arriving on international flights, which failure resulted in delays in admitting international travelers in several U.S. airports, including those in Miami, New York, and San Francisco.

Complaint, Ex. B. Plaintiff requested expedited processing of his FOIA request because "it pertains to a matter about which there is an 'urgency to inform the public concerning actual or alleged Federal Government activity,' and the request is made by a person 'primarily engaged in disseminating information.'" *Id.* (quoting 5 U.S.C. § 552).

On September 23, 2005, plaintiff received a phone call from Erlinda Byrd, a CBP official in the CBP's Office of Public Affairs. *See* Poulsen Decl. ¶ 7. Ms. Byrd told plaintiff that CBP would prefer if plaintiff voluntarily withdrew his FOIA request, stating that CBP officials did not want to go to the trouble of conducting a records search that, in their view, would produce no information that they would be inclined to release, except for information that had already been released to the public and reported in the news. *Id.* Plaintiff refused to withdraw his request. *Id.*

Plaintiff called CBP on December 9, 2005 to inquire regarding the status of his FOIA request. *Id.* at ¶ 8. Plaintiff was told that his request had been forwarded to the Office of Information and Technology and was directed to that office. *Id.* Plaintiff then spoke with CBP official Diane Hundertmark, who told him that the Office of Information and Technology did not have his request. *Id.* After this conversation, plaintiff wrote a follow-up letter to CBP dated December 9, 2005, explaining that he had still not received responses to his requests and relating the details of his conversations with CBP employees. *Id.* at ¶ 9; Ex. C.

On December 15, 2005, CNET News.com published an article that addressed the August 18, 2005 CBP computer failure. *Id.* at ¶ 10; Ex. D. The article quotes a Homeland Security Department spokesman who said about the computer failure, "They have computer glitches from time to time due

to the complexity of the system, and they're not a frequent thing, but they do happen on occasion, and that was one instance of it." *Id.* at Ex. D. The article reported that according to the spokesman, the computer failure was not due to a computer virus as had initially been reported. *Id.*

On January 31, 2006, plaintiff received an undated letter from the Office of Information and Technology, signed by Diane Hundertmark. *Id.* at ¶ 12; Ex. E. The letter states,

> Your request for additional documentation related to the U.S. Customs and Border Protection computer system outage of August 18, 2005 as reported by the Associated Press and other media outlets such as the Miami Herald has been reviewed and considered. It has been determined that additional information pursuant to the incident beyond what has already been provided to the media is exempt from disclosure in its entirety pursuant to 5 U.S.C. § 552(b)(2), as it is related solely to the internal administrative practices of the agency.

Id. at Ex. E. By letter dated February 2, 2006, plaintiff appealed the CBP's determination on five grounds: (1) CBP had wrongfully withheld records because 5 U.S.C. § 552(b)(2) does not apply; (2) CBP had failed to provide information that was already publicly known; (3) CBP did not conduct an adequate search for records; (4) CBP failed to comply with time limits in processing plaintiff's FOIA request; and (5) CBP did not respond to plaintiff's request for expedited processing. *Id.* at Ex. F.

Plaintiff filed this action on March 7, 2006 after he did not receive a response to his appeal. *Id.* at ¶ 14. After filing this action, CBP provided plaintiff with six pages of heavily-redacted responsive documents on March 31, 2006. *Id.* at Ex. G. The documents consist of the following: (1) a two page document titled "CBP Worm 08/18/05: Executive Summary"; (2) a two page document titled "CBP Worm (Zotob) on August 18, 2005: Executive Summary"; (3) one entirely redacted one page document; and (4) a one page document titled "Detail of Microsoft Vulnerability Notification." *Id.* CBP did not provide plaintiff an explanation of why portions of the documents were redacted. *Id.* at ¶ 17.

LEGAL STANDARD

Summary adjudication is proper when "the pleadings, depositions, answers to interrogatories, and admissions on file, together with affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law." Fed. R. Civ. P. 56(c). In a motion for summary judgment, "[if] the moving party for summary judgment meets its initial burden of identifying for the court those portions of the materials on file that it believes demonstrate the

absence of any genuine issues of material fact, the burden of production then shifts so that the non-moving party must set forth, by affidavit or as otherwise provided in Rule 56, specific facts showing that there is a genuine issue for trial." *T.W. Elec. Service, Inc., v. Pac. Elec. Contractors Association*, 809 F.2d 626, 630 (9th Cir. 1987) (citing *Celotex Corporation v. Catrett*, 477 U.S. 317 (1986)).

In judging evidence at the summary judgment stage, the Court does not make credibility determinations or weigh conflicting evidence, and draws all inferences in the light most favorable to the non-moving party. *See T.W. Electric*, 809 F.2d at 630-31 (citing *Matsushita Elec. Indus. Co., Ltd. v. Zenith Radio Corp.*, 475 U.S. 574 (1986)); *Ting v. United States*, 927 F.2d 1504, 1509 (9th Cir. 1991). The evidence presented by the parties must be admissible. Fed. R. Civ. P. 56(e). Conclusory, speculative testimony in affidavits and moving papers is insufficient to raise genuine issues of fact and defeat summary judgment. *See Thornhill Publ'g Co., Inc. v. GTE Corp.*, 594 F.2d 730, 738 (9th Cir. 1979).

It is generally recognized that summary judgment is a proper avenue for resolving a FOIA claim. *See National Wildlife Federation v. United States Forest Service*, 861 F.2d 114 (9th Cir. 1988). The government agency bears the ultimate burden of proving that a particular document falls within one of the nine statutory exceptions to the disclosure requirement. *See Dobronski v. FCC*, 17 F.3d 275, 277 (9th Cir. 1994). The government may submit affidavits to satisfy their burden, but "the government 'may not rely upon conclusory and generalized allegations of exemptions.'" *Kamman v. IRS*, 56 F.3d 46, 48 (9th Cir. 1995) (*quoting Church of Scientology v. Department of the Army*, 611 F.2d 738, 742) (9th Cir. 1980)). The government's "affidavits must contain 'reasonably detailed descriptions of the documents and allege facts sufficient to establish an exemption.'" *Id*. (*quoting Lewis v. IRS*, 823 F.2d 375, 378 (9th Cir. 1987)).

DISCUSSION

1. CBP Officials Conducted an Adequate Search

The parties dispute whether CBP officials conducted an adequate search for records responsive to plaintiff's FOIA request. Plaintiff seeks an order finding that CBP's personnel acted arbitrarily and capriciously in withholding documents, and referring the matter to a Special Counsel who "shall

promptly initiate a proceeding to determine whether disciplinary action is warranted against the officer or employee who was primarily responsible for the withholding." 5 U.S.C. § 552 (a)(4)(F). The Court DENIES this aspect of plaintiff's motion and concludes that defendant's search was adequate.

Defendant has submitted two declarations by Shari Suzuki which detail the steps that CBP took in response to plaintiff's FOIA request. Ms. Suzuki is the Chief of the Freedom of Information Act Appeals, Policy & Litigation Branch ("FAPL"). Suzuki Decl. ¶ 1. According to Ms. Suzuki, plaintiff's August 22, 2005 letter was received by the FAPL Branch and forwarded to the Office of Information and Technology ("OIT") on September 8, 2005, but OIT did not receive plaintiff's letter. *Id.* at ¶¶ 6-7. Ms. Suzuki states she believes the request was misdirected to the Office of Public Affairs. Supp. Suzuki Decl. ¶ 13.

The FAPL Branch received plaintiff's December 9, 2005 letter inquiring about the status of his FOIA request on December 19, 2005. Supp. Suzuki Decl. ¶ 14. FAPL forwarded that letter to OIT on December 29, 2005, and OIT received plaintiff's FOIA request on December 30, 2005. *Id.* at ¶¶ 14-15. OIT conducted a search for records responsive to the FOIA request during the week of January 10, 2006. Suzuki Decl. ¶ 9.

According to Ms. Suzuki, OIT searched more than 200,000 records in three different systems for information pertaining to plaintiff's request. *Id.* at ¶ 11. The three systems searched are (1) a database that tracks calls to the OIT help desk (CBP employees can call the help desk if they experience problems with their desktop computers); (2) a database that tracks "work tickets" (OIT generates a work ticket when it performs work in response to a call to the help desk); and (3) a limited access local area network (LAN) shared drive for weekly status reports or other documents. Suzuki Decl. ¶ 11. OIT personnel searched the two databases using a date range around the time of the incident (August 1 to August 30, 2005), and the search included the search terms "Zotob," "US Visit,"[1] "virus," and "Miami." *Id.* OIT personnel also searched the LAN drive for any other documents related to the incident,

[1] The US Visit Program is part of the U.S. Department of Homeland Security. The US Visit workstations were the primary target of the virus.

including OIT weekly status reports[2] for August and September 2005. *Id.* After locating the relevant weekly status reports, OIT personnel manually reviewed the reports for any information related to the incident. *Id.* Suzuki states that while the help desk and "work ticket" databases are limited in nature, the LAN drive is "expansive in nature and contains a large number of varied documents," including correspondence with other offices within CBP. Supp. Suzuki Decl. ¶ 8. Ms. Suzuki was advised that OIT located fifteen responsive documents, totaling 672 pages. *Id.* at ¶ 12. OIT determined that the documents were exempt from disclosure pursuant to 5 U.S.C. § 552 (b)(2), (b)(6), (b)(7)(C), and (b)(7)(E).

Plaintiff contends that CBP's search was inadequate because it did not search OIT e-mail. Plaintiff contends that e-mail correspondence, properly redacted to protect the privacy of recipient and sender, could add important details to the public debate which entries in a database, or memos to thousands of workers, cannot. Suzuki's supplemental declaration responds that CBP employees are not likely to use e-mail to seek help regarding computer problems via e-mail, and instead generally call the help-desk. Supp. Suzuki Decl. ¶ 8.

Plaintiff also complains that CBP did not search any databases that revealed inter- or intra-agency correspondence about the Zotob infection. Plaintiff asserts that in light of the significant disruption that resulted from the Zotob infection, it is exceedingly unlikely that there would not be any correspondence between OIT and other CBP offices, or between CBP and other agencies within DHS. Plaintiff contends that this is particularly so because the US-VISIT program is by nature a collaboration between multiple agencies, and is overseen by a separate "US-VISIT Program Office" within DHS. Plaintiff contends that inter-agency memos about the computer problem would likely shed light on the cause of the outage and whether and how it was fixed. However, according to the Supplemental Suzuki declaration, the LAN drive searched by CBP personnel did contain memos between offices within CBP, and in fact the two redacted executive summaries produced to plaintiff are such memos. Supp. Suzuki Decl. ¶¶ 5-8.

---

[2] Suzuki states that weekly status reports are submitted to the Commissioner of CBP and senior staff. Supp. Suzuki Decl. ¶ 7. These reports are used by CBP offices to highlight significant activity to the Commissioner of CBP and other offices, and are a means of communication between offices. *Id.*

In responding to a FOIA request, an agency must "demonstrate that it has conducted a 'search reasonably calculated to uncover all relevant documents.'" *Zemansky v. E.P.A.*, 767 F.2d 569, 571 (9th Cir. 1985) (quoting *Weisberg v. United States Dep't of Justice*, 745 F.2d 1476, 1485 (D.C. Cir. 1984)). "The adequacy of the agency's search is judged by a standard of reasonableness, construing the facts in the light most favorable to the requestor." *Citizens Comm'n on Human Rights v. Food & Drug Admin.*, 45 F.3d 1325, 1328 (9th Cir. 1995). "[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*." *Zemansky*, 767 F.2d at 571 (emphasis in original).

In order to demonstrate the adequacy of a search, "the agency may rely upon reasonably detailed, nonconclusory affidavits submitted in good faith." *Id.* (*quoting Weisberg v. United States Dep't of Justice*, 745 F.2d at 1485)). The Court concludes that CBP's search was adequate based upon the detailed description of the search contained in the two Suzuki declarations. Defendant has demonstrated that searching over 200,000 records in three different systems for information pertaining to plaintiff's request was "a search reasonably calculated to uncover all relevant documents." *Id.* (quotations omitted). Moreover, one of the databases searched contains internal memoranda of the sort plaintiff is seeking. Because the issue to be resolved is the adequacy of the search and "not whether there might exist any other documents," the Court finds that the number of records searched within the time frame of the incident was both thorough and reasonable. *Id.*[3]

2. Exemptions

CBP asserts that the 15 withheld documents, consisting of 666 pages, are largely exempt because

[3] At oral argument plaintiff asserted that defendant should have searched broader dates, including the dates up until the time the search was conducted in January 2006. However, the Court concludes that defendant's search of the dates around the time of the incident was adequate because it is reasonable to assume that most, if not all, relevant documents would have been created in August and September 2005 when the virus impacted the computers and when CBP addressed the problem. There has been no suggestion that the virus continued to affect CBP computers through January 2006.

(1) they were compiled for law enforcement purposes; (2) they were withheld for privacy reasons[4]; and/or (3) they relate solely to the internal personnel rules and practices of the CBP. Plaintiff does not dispute that the government properly withheld the fifth, sixth, seventh and ninth documents. Reply at 4-5. This order addresses whether the remaining documents, or portions therein, are exempt.

A. Exemption 7

Exemption 7 shields from public disclosure agency information where: (1) the "information [was] compiled for law enforcement purposes," and (2) "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E). "The burden is placed upon the government agency to establish that a given document is exempt from disclosure." *Church of Scientology*, 611 F.2d at 742; *see also Gordon v. Federal Bureau of Investigation*, 390 F. Supp. 2d 897, 901 (N.D. Cal. 2004).

The first question in determining the applicability of Exemptions 7(E) is whether "the withheld record was compiled for law enforcement purposes." *See Rosenfeld v. United States Dep't. of Justice*, 57 F.3d 803, 808 (9th Cir. 1995). "An agency which has a clear law enforcement mandate, such as the FBI, need only establish a 'rational nexus' between enforcement of a federal law and the document for which an exemption is claimed." *Church of Scientology*, 611 F.2d at 748. The parties agree that CBP has a clear law enforcement mandate, but dispute whether the records at issue bear a rational relationship to the agency's law enforcement function. Plaintiff contends that the computer repair records were created to track the performance of CBP's computer system, not to enforce any border protection laws. Defendant argues that the computer files at issue are used to substantially assist CBP with its law enforcement purpose because the documents were compiled to repair CBP's computer network, which in turn is used to enforce border security.

The Court agrees with plaintiff that the requested documents do not have a rational nexus with

[4] Because plaintiff does not contest defendant's withholding of names, phone numbers, and other personal identifying information of CBP employees under "Exemption 6," 5 U.S.C. § 552(b)(6), the Court does not address defendant's arguments on these matters.

CBP's law enforcement mandate. The connection between the documents and CBP's law enforcement mandate is so attenuated that, according to defendant, virtually any document created by CBP would be "compiled for law enforcement purposes." However, "[i]n determining whether a 'law enforcement purpose' is present, courts must look to the purpose behind the compilation of the document." *Id*. Here, the documents were generated as a matter of course in response to the computer virus; the documents were not created as part of an investigation, or in connection with CBP's enforcement of a federal law. Accordingly, the Court finds that the documents are not exempt under § 552 (b)(7).

B. Exemption 2

The government has also invoked exemption 2 to justify its withholding of documents. Exemption 2 prevents public disclosure of information "related solely to the internal personnel rules and practices of an agency." 5 U.S.C.§ 552(b)(2). "Exemption 2 is not applicable to matters subject to such a genuine and significant public interest," so long as "the situation is not one where disclosure may risk circumvention of agency regulation. . . ." *Department of Air Force v. Rose*, 425 U.S. 352, 369 (1976). The general purpose of exemption 2 is "simply to relieve agencies of the burden of assembling and maintaining for public inspection matter in which the public could not reasonably be expected to have an interest." *Id*. at 369-70.

A "high 2" exemption protects "[p]redominantly internal documents the disclosure of which would risk circumvention of agency statutes and regulations." *Schiller v. N.L.R.B.*, 964 F.2d 1205, 1207 (D.C. Cir. 1992); *see also Nat'l Treasury Employees Union v. United States Customs Serv.*, 802 F.2d 525, 530-31 & n.19 (D.C. Cir. 1986). The "low 2" exemption protects "[p]redominantly internal documents that deal with trivial administrative matters" with little public interest. *Schiller*, 964 F.2d at 1207. Defendant argues that the "low 2" exemption is properly applied to all trivial administrative data, including identification numbers and computer codes, and that the remaining information is "high 2" information that is predominantly internal and would provide a roadmap for future criminals to circumvent the CBP computer system. Plaintiff asserts that certain withheld information falls under neither the "low 2" nor the "high 2" exemption, and should be released in order to inform the public about the CBP computer shutdown.

As described in greater detail below, the Court concludes that some of the information withheld by defendant qualifies as "high 2" or "low 2" material, and thus was properly withheld. In general, the Court finds that specific information about how CBP repaired the computers, such as the precise patch used, or detailed information about future remediation efforts, was properly withheld as "high 2" material because the disclosure of such information could make the CBP computer system vulnerable to future attacks. *See Wilson v. Drug Enforcement Admin.*, 414 F. Supp. 2d . 5, 12 (D.D.C. 2006) (internal codes classifying drug violators fall under exemption 2 because "[w]ith such information, a suspect could change his pattern of drug trafficking in order to avoid detection and apprehension.").

In addition, other information of a purely trivial, administrative nature, such as "incident i.d." numbers, codes assigned to particular machines, and which CBP employees were involved in the repair, was properly withheld as "low 2" material because there is no significant public interest in such information. *See id.*; *see also Schiller*, 964 F.2d at 1208 ("[I[nternal time deadlines and procedures, recordkeeping directions, instructions on which agency officials to contact for assistance, and guidelines on when clearance from [other departments] is necessary for certain decisions" are "housekeeping matters appropriately withheld under [E]xemption 2.").

However, the Court finds that defendant improperly withheld descriptive information regarding the scope of the incident, such as the numbers or percentages of computers infected or the different cities reporting problems, or general accounts of the problem and the remedy, such as statements that a virus infected various computers and that patches were installed. This information is of interest to the public, and defendant has failed to meet its burden of showing that exemption 2 applies to this material. Although defendant repeatedly asserts that this information would render the CBP computer system vulnerable, defendant has not articulated *how* this general information would do so. *Cf. Gordon v. Federal Bureau of Investigation*, 388 F. Supp. 2d 1028, 1037 (N.D. Cal. 2005) (documents explaining FBI's creation of aviation watch lists exempt because such information might assist terrorists, but documents explaining the legal basis for detaining a person not exempt because the FBI failed to explain how such information could be used to circumvent the law). To the extent such information is reasonably segregable, defendant must disclose it.

C. Specific Findings

The Court has reviewed *in camera* the documents at issue in conjunction with the Suzuki declarations, and makes the following specific findings regarding the application of exemption 2:

(1) Document One

Document one is a spreadsheet report which reflects all responsive records located in the helpdesk calls database. Suzuki Decl. ¶ 15. According to defendant, this document provides a summary of each call received by the helpdesk related to the incident at issue. *Id.* Plaintiff argues that such information would provide a public understanding of the impact of the computer virus. Plaintiff asks for the disclosure of the following columns: "open.time," "Solved by Level," "Status," "Brief Description," and "Resolution."

The Court concludes that all information contained in these columns should be released except the following: (1) identifying codes for machines and workstations; (2) names of CBP employees; and (3) names or other specific identifying information for databases or the patch installed. The remaining information contained in these columns should be disclosed because it sheds light on the scope and nature of the problem without divulging material that would render the CBP system vulnerable.

(2) Document Two

The second document consists of all the call records contained in the helpdesk database and totals 330 pages. Suzuki Decl. ¶ 16. While the first document is the summary report of calls received regarding the incident, document two contains the actual call records – which are computer printouts – created in response to calls to the helpdesk. *Id.* The Court concludes that this document contains largely "low 2" information, such as unique identifying codes for machines, call identification numbers, names and other personal identifying information of CBP employees and contractors, as well as some "high 2" information such as the specific name of the patch installed. The Court further finds that the exempt material is inextricably intertwined with non-exempt information, and thus that defendant

properly withheld this document in full.[5]

(3) Document Three

Document three is a spreadsheet report which reflects all responsive records located in the work ticket database. Suzuki Decl. ¶ 17. Plaintiff requests the following columns to be disclosed: "Reported By City," "Category," "Priority," "Status," "Date Opened," "Last Update," "Brief Description," and "Resolution." Aside from the information described above in connection with document one (such as identifying codes for machines and workstations; names of CBP employees; and names or other specific identifying information for databases or the patch installed), defendant has not articulated why the other information is exempt. For example, defendant has failed to demonstrate why disclosure of the "Reported by City" category would compromise CBP's infrastructure. The Court concludes that defendant must disclose all information contained in the eight categories listed above, with the exception of appropriate redactions for the exempt material listed *supra*.

(4) Document Four

Document four consists of the work tickets contained in the work ticket database and totals 244 pages. Suzuki Decl. ¶ 18. While document three is the summary report of work tickets, document four contains the actual work tickets – computer printouts – created in response to calls to the database. *Id.* For the same reasons as set forth above with regard to document two, the Court concludes that document four contains largely "high 2" and "low 2" information that is inextricably intertwined with non-exempt material.

(5) Document Eight

Document eight is a Zotob Status Meeting Notice consisting of two pages. This document was used to set up an internal OIT meeting on November 11, 2005 regarding the Zotob virus, and it discusses

[5] Moreover, plaintiff's interest in disclosure of document two is less compelling in light of the fact that much, if not all, of the non-exempt information that plaintiff seeks in document two is contained in document one.

the feasibility of various future remediation options. Suzuki Decl. ¶ 21. The document includes the names of attendees, a list of agenda items, and specific information about remediation options. The Court concludes that document eight is a combination of "low 2" administrative, trivial information and "high 2" material that could compromise CBP's systems. *See Judicial Watch Inc. v. U.S. Dep't of Commerce*, 337 F. Supp. 2d 146, 166 (D.D.C. 2004) (cases, file numbers and other administrative markings fell under exemption 2 because "knowledge of this information may render the Customs Service's electronic records system vulnerable to hacking, and facilitate circumvention of the laws and regulations enforced by the Customs Service.").

(6) Documents Ten and Eleven

Documents ten and eleven are from the CBP internal website. Suzuki Decl. ¶ 23. According to defendant, these documents "are similar to a case history documenting the technical distribution of the security patch employed in the instant incident." *Id*. The Court finds that these documents are similar to "an internal checklist of clerical actions, [and] code numbers" and are "lacking in any genuine or significant public benefit," and are thus exempt under "low 2." *DiPietro v. Executive Office of U.S. Attys*, 368 F. Supp. 2d 80, 82 (D.D.C. 2005).

(7) Document Twelve

Document twelve is a message to duty officers dated August 17, 2005 and consists of two pages. Suzuki Decl. ¶ 24. According to defendant, this document "was created to give duty officers at the helpdesk or security center a brief overview of the event relative to the Zotob worm and the steps to be taken by CBP in responding to the threat." *Id.*

The Court concludes that to the extent this document generally describes what occurred when the virus affected CBP's computers – as opposed to the specific measures CBP took in response or specific information about how CBP's computer systems are structured – such information is not exempt and should be disclosed. For example, the statement that "Multiple worms targeting newly announced flaws in Microsoft's Windows operating system are circulating on the Internet including the Zotob

worm that has received the most press"[6] is neither low 2 nor high 2 material. Defendant shall produce document twelve subject to the following redactions: (1) in the first paragraph, the third sentence beginning "CBP currently runs . . . ."; (2) in the first paragraph, the sentence beginning "The identified hotfix from Microsoft . . . ." and all remaining sentences in that paragraph; (3) under the section titled "Current Status," the third paragraph beginning "All CBP . . . .", and the remainder of the document.

(8) Document Thirteen

Document thirteen is a compilation of relevant portions of OIT weekly status reports and consists of two pages. *Id.* at ¶ 25. This document highlights security actions taken by CBP in response to the incident. *Id.* The Court concludes that the majority of this document is "high 2" material because it sets forth the specific measures CBP took in response to the worm, and the disclosure of this information could render CBP's systems vulnerable to future attack. *See Judicial Watch Inc.*, 337 F. Supp. 2d at 166. However, the first paragraph of the document under the section "South Florida Circuit Outage" does not contain exempt information because it simply describes the incident in general terms, and accordingly should be produced.

(9) Documents Fourteen and Fifteen

Documents fourteen and fifteen are executive summaries providing a narrative overview of the incident and summarizing the technical data contained in the other responsive documents. Suzuki Decl. ¶ 26. Defendant produced these documents with extensive redactions. The Court finds that some of the redacted material was simply descriptive information regarding the incident that is not exempt. For example, on page one of document fourteen, defendant redacted the statement, "It was identified that the USVISIT workstations would still need to be patched in order to prevent exposure within the CBP environment." Defendant has not articulated any reason why such basic, non-specific information should be exempt; it is not surprising that a computer network would be significantly affected by a

[6] This is the first sentence in the paragraph under "Virus Executive Review" in document twelve.

computer virus and that the computers would require repairs.[7] Such information is general enough in nature that it would not "risk circumvention of agency regulation. . . ." *Rose*, 425 U.S. at 369. Such information is also not trivial "low 2" information, but rather important to the public's understanding of the system outage.[8]

Accordingly, defendant shall re-release document fourteen but may only retain the following redactions:

- All references to the specific name of the software used and the code associated with the patch;
- The words after "USVISIT" in the third sentence in the 08/17/05 entry;

The redactions in the 08/18/05 2130 entry;

- The redactions in the last four sentences in the 08/18/05 2355 entry;
- The redactions in the 8/19/05 0030entry;
- The redactions in the 8/19/05 0200 entry except for the number of machines;
- The name and contact information of the staff member at the bottom of page two.

Document fifteen contains much of the same language as document fourteen; to the extent that the language is identical or substantially similar, defendant shall re-produce document 15 subject to the same redactions set forth above.[9] In addition, the following information in document fifteen should remain redacted:

- The last sentence in paragraph two;

---

[7] Defendant also redacted innocuous words such as "contacted," as well as general percentages and numbers describing the effect of the virus upon the workstations.

[8] In addition, at times defendant's redactions are inconsistent. For instance, the sentence "USVISIT workstations were not targeted for distribution as part of this initial distribution" was not redacted in document fourteen, while the identical sentence was redacted in document fifteen. Similarly, the phrase "normal desktop workstations" was not redacted in document fourteen but in document fifteen, page one, line two, the same phrase was redacted. Defendant also sometimes redacted the name "USVISIT" and other times left it unredacted. Again, in document fourteen, page one, line ten, the title "Duty Officer" was redacted, yet in document fifteen, page one, line ten, the same title was not redacted. Similarly, "Operations Staff" was redacted in document fourteen but not in document fifteen.

[9] For example, document fourteen states "the previously defined worm" while document fifteen states "the previously identified worm."

- The last two words in paragraph four;
- The fifth and sixth paragraphs, which are contained under the first bolded subsection;
- The redactions in paragraph 1 of the "FAQs" subsection may remain except that numbers and percentages should not be redacted, nor should "FAQs" be redacted;
- In paragraph 2 of the "FAQs" subsection, the second sentence.
- The second sentence in the 08/17/2005 entry under the "Incident Timeline" section, on page three;
- The information found under the "Action Items" subsection.

CONCLUSION

For the foregoing reasons and for good cause shown, the Court hereby GRANTS in part and DENIES in part defendant's motion for summary judgment, and GRANTS in part and DENIES in part plaintiff's motion for summary judgment. (Docket Nos. 9, 19). Defendant shall produce the additional unredacted material by **October 6, 2006**.

IT IS SO ORDERED.

Dated: September 25, 2006

SUSAN ILLSTON
United States District Judge