UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

JUDICIAL WATCH INC.,	
Plaintiff,	
v.	
UNITED STATES SECRET SERVICE,	Civil Action No. 06-310 (RMC)
Defendant.	

DEFENDANT'S SUPPLEMENTAL MOTION FOR SUMMARY JUDGMENT

Pursuant to Federal Rule of Civil Procedure 56, defendant hereby moves for summary judgment. The basis for this motion is set forth in the attached memorandum.

Dated: November 30, 2007

Respectfully submitted,

JEFFREY S. BUCHOLTZ
Acting Assistant Attorney General

JEFFREY A. TAYLOR
United States Attorney

CARL J. NICHOLS
Deputy Assistant Attorney General

JOSEPH H. HUNT
Branch Director

ELIZABETH J. SHAPIRO
Assistant Branch Director

s/ Justin M. Sandberg
JUSTIN M. SANDBERG
(Ill. Bar. No. 6278377)

OF COUNSEL:

LIZA MURPHY
MOLLY WEBER

United States Secret Service

Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W. #7224
P.O. Box 883 Ben Franklin Station
Washington, D.C. 20044
Telephone: (202) 514-3489
Facsimile: (202) 616-8202
E-mail: justin.sandberg@usdoj.gov

Attorneys for Defendant

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

JUDICIAL WATCH INC., Plaintiff, v. UNITED STATES SECRET SERVICE, Defendant.	Civil Action No. 06-310 (RMC)

MEMORANDUM IN SUPPORT OF SUPPLEMENTAL MOTION FOR SUMMARY JUDGMENT

INTRODUCTION

Pursuant to the Court's minute entry providing defendant until November 30, 2007 to supplement its filings, defendant files its Supplemental Motion for Summary Judgment and this supporting memorandum. Plaintiff and defendant entered into a Joint Stipulation and Agreed Order pursuant to which defendant pledged to produce responsive documents by May 10, 2006.[1] Joint Stipulation and Agreed Order, April 25, 2006 ("Joint Stipulation"), Doc. No. 8. Following a reasonable search, defendant produced all responsive records that it had found. Since defendant conducted its original search and document production (and the related follow-up

[1] The Secret Service assumes that the records it has searched and produced are "agency" records, as that term is used in the Freedom of Information Act ("FOIA"), solely for the purposes of its motions to dismiss and its supplemental motion for summary judgment; it does not otherwise concede, through its use of the word "responsive" or otherwise, that the records it has searched or produced are agency records, as opposed to records governed by the Presidential Records Act, 44 U.S.C. § 2201 et seq. To that end, records have been released to plaintiff solely as a discretionary matter.

searches and document production which it has already documented), it has identified as potentially responsive other categories of records, including a type of record known as "Sensitive Security Records."[2] Setting aside the Sensitive Security Records, defendant has supplemented its prior searches with an additional comprehensive search and has found no additional responsive records. As for the Sensitive Security Records, defendant can neither confirm nor deny that it has any Sensitive Security Records responsive to this FOIA request. The simple act of doing so, particularly in a FOIA case in which plaintiff seeks records of only one individual, would reveal sensitive information about the methods used by the Secret Service to carry out its protective function. Even if any responsive records exist, they would be exempt from disclosure pursuant to FOIA Exemptions 2, 7(E), and 7(F) (5 U.S.C. §§ 552(b)(2), (b)(7)(E), and (b)(7)(F)) because they contain information that, if released, would impinge on defendant's ability to fulfill its protective duties.

The Court should enter summary judgment in favor of defendant. There is no question of material fact regarding defendant's compliance with the FOIA: Defendant has demonstrated (through this and prior filings) that all responsive, non-exempt records have been released to plaintiff following a reasonable search and that any responsive Sensitive Security Records would be exempt from disclosure.

---

[2] Sensitive Security Records relate to the background investigations and security process sometimes undertaken in connection with a visit to the White House Complex. Second Declaration of Paul S. Morrissey, November 30, 2007 ("Second Morrissey Decl."), ¶ 3 (attached as Exhibit 1); Declaration of Craig W. Ulmer, November 30, 2007 ("Ulmer Decl."), ¶ 10 (attached as Exhibit 2). In Citizens for Responsibility and Ethics in Washington v. Dep't of Homeland Security, 06-CV-1912 (RCL), defendant refers to these records as "Additional Security-Related Records." See Defendant's Motion for Summary Judgment, 06-CV-912, May 25, 2007, at 9, Doc. No 29.

BACKGROUND

By a letter dated January 20, 2006, plaintiff submitted a FOIA request seeking "all agency records concerning, relating to, or reflecting * * * [a]ll White House visitor logs from January 1, 2001 to present that reflect the entries and exit(s) of lobbyist Jack Abramoff from the White House." Freedom of Information Act Request, January 20, 2006 ("FOIA Request"), at 1 (attached as Exhibit 2 to plaintiff's Motion to Compel Defendant United States Secret Service to Comply with This Court's Order and for Sanctions, May 16, 2006 ("Motion to Compel"), Doc. No. 12). About three months later, plaintiff and defendant entered into a stipulation which was endorsed by the Court. See Joint Stipulation. In the Joint Stipulation, Defendant agreed to produce responsive documents "without redactions or claims of exemption" by May 10, 2006. Id. ¶ 2. By that deadline, defendant conducted a reasonable search and released to plaintiff all known responsive records. Defendant's Memorandum in Support of Motion to Dismiss for Lack of Subject Matter Jurisdiction, May 16, 2006 ("Memo."), Doc. No. 14. Shortly thereafter, defendant supplemented its prior document production by releasing several more responsive records.[3] Defendant's Reply in Support of Its Motion to Dismiss for Lack of Subject Matter Jurisdiction, July 7, 2006 ("Reply"), Doc. No. 22. The records released comprised Worker and Visitor Entrance System ("WAVES") data and Access Control Records System data ("ACR"), which generally speaking record visits by individuals to the White House Complex (also "Complex"), and which were described in detail in the Declaration of Kathy J. Lyerly, May 16,

[3] Defendant also filed a declaration in December 2006 describing additional potentially relevant categories of records that it had identified. Declaration of Paul S. Morrissey, December 12, 2006 ("Morrissey Decl.") (attached to Notice of Filing, December 12, 2006, Doc. No. 31). Though it was not clear whether the records in these categories were responsive, defendant searched them. Id. ¶ 4. No responsive records were located. Id.

2006 ("Lyerly Decl."), ¶ 8 (attached to Memo.), and the Second Declaration of Kathy J. Lyerly, July 7, 2006 ("Second Lyerly Decl."), ¶¶ 15, 16 (attached as Exhibit 1 to Reply).

After defendant conducted its original search and released records to plaintiff, it lodged a motion to dismiss for lack of jurisdiction. Motion to Dismiss for Lack of Subject Matter Jurisdiction, May 16, 2006, Doc. No. 14. In the memorandum filed in support of this motion, defendant demonstrated that plaintiff's FOIA claim was moot because, as defendant had released all responsive, non-exempt records found after a reasonable search, plaintiff had "obtained everything that [it] could recover . . . by a judgment of th[e] court in [its] favor," Hall v. CIA, 437 F.3d 94, 99 (D.C. Cir. 2006) (internal quotations omitted). See Memo. at 4; see also Tijerina v. Walters, 821 F.2d 789, 799 (D.C. Cir. 1987) (concluding that the case was moot because the agency had released all responsive, non-exempt records to plaintiff).

In the course of reviewing potentially responsive records for a different FOIA case, defendant has identified as potentially responsive several categories of records that were not addressed in previous filings in this case, including Sensitive Security Records. Leaving aside Sensitive Security Records, in an abundance of caution, as noted earlier, defendant searched these records and found no responsive records. With respect to Sensitive Security Records, these documents are highly sensitive records relating to the background investigation and security process undertaken in connection with certain visits to the White House Complex. Second Morrissey Decl. ¶ 3; Ulmer Decl. ¶ 10. These records are created in the course of conducting additional background checks and other security-related activities regarding certain visitors, who are chosen based on certain details in their backgrounds and/or the circumstances of their visits. Second Morrissey Decl. ¶ 3; Ulmer Decl. ¶ 10. Included in these records are the names and other

identifying information concerning such visitors (including, in some cases, their birth dates and/or Social Security numbers) and background information on them or information regarding their visits to the Complex, which may include criminal history and/or other security-related information. Second Morrissey Decl. ¶ 3; Ulmer Decl. ¶ 10.

ARGUMENT

THE COURT SHOULD ENTER SUMMARY JUDGMENT IN FAVOR OF DEFENDANT

The Court should enter summary judgment in favor of defendant, as there is no material question of fact regarding its compliance with FOIA: Defendant produced all responsive, non-exempt documents found after a reasonable search, and any responsive Sensitive Security Records would be exempt from disclosure. "To obtain summary judgment in a FOIA action, an agency must show, viewing the facts in the light most favorable to the requester, that there is no genuine issue of material fact as to the agency's compliance with FOIA." Smith v. Environmental and Natural Resources Division, 2007 4127647, at * 1 (D.D.C. 2007) (citing Steinberg v. U.S. Dept. of Justice, 745 F.2d 1467, 1485 (D.C. Cir. 1994)). To comply with the FOIA and, by extension, to be entitled to summary judgement, the agency must demonstrate that it conducted a reasonable search. See Truitt v. Dep't of State, 897 F.2d 540, 542 (D.C. Cir. 1990). And if the agency withholds any documents, the Court may enter judgment when the agency's declarations establish "the justifications for nondisclosures 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." Military Audit Project v. Casey, 656 F.2d 724, 738 (D.C. Cir. 1981).

I. Defendant Conducted A Reasonable Search

Defendant conducted a reasonable search by the May 10, 2006 deadline set out in the Joint Stipulation. Using qualified personnel and appropriate methods, defendant searched all visitor logs then identified by defendant as potentially responsive. See First Lyerly Decl. ¶ 9, 12-13; Second Lyerly Decl. ¶¶ 6, 13. Defendant has already demonstrated the reasonableness of its initial search in prior filings, see First Lyerly Decl. ¶ 9, 12-13; Second Lyerly Decl. ¶¶ 6, 13, and it need not rehash that issue in full here. Importantly, though, the current revelation of the Sensitive Security Records (and other records) does not undermine that showing. Rather, defendant's conduct underscores the integrity of its search process and the seriousness with which it takes its obligations: Defendant has continued to apprise plaintiff and the Court of potentially responsive documents even after conducting a reasonable search.

The reasonableness of a search is measured by the appropriateness of the methods used, not its results. Iturralde v. Comptroller of Currency, 315 F.3d 311, 315 (D.C. Cir. 2003); Meeropol v. Meese, 790 F.2d 942, 953 (D.C. Cir. 1986) (holding that "a search [was] not unreasonable simply because it fail[ed] to produce all relevant material" as "[i]t would be unreasonable to expect even the most exhaustive search to uncover *every* responsive file") (emphasis in parenthetical statement in original). An agency is required to make "a good faith effort to conduct a search for the requested records, using methods 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). An agency need not search every file where a responsive document could possibly exist for its search to be reasonable; the reasonableness of the search is measured in light of the

totality of the circumstances. See Safecard Servs., Inc. v. SEC, 926 F.2d 1197, 1201 (D.C. Cir. 1991).

Defendant conducted its original search using reasonable methods. To find responsive records, defendant searched the records that then had been identified as memorializing visits to the White House Complex – WAVES and ACR records. See First Lyerly Decl. ¶ 9, 12-13; Second Lyerly Decl. ¶¶ 6, 13; Second Morrissey Decl. ¶ 4. Defendant did not initially identify Sensitive Security Records as being potentially responsive. See Second Morrissey Decl. ¶ 4. The primary purpose of Sensitive Security Records, after all, is not to track those who visit the White House, but to facilitate additional background checks and other security-related activities with regard to certain individuals who visit the Complex.[4] See Second Morrissey Decl. ¶ 3; Ulmer Decl. ¶ 10. That said, after many months of litigating other similar FOIA cases, defendant decided to treat these records as possibly "relating" to visits to the White House. See Second Morrissey Decl. ¶ 4; FOIA Request at 1. Once defendant decided to treat records like the Sensitive Security Records as potentially responsive, it conducted a comprehensive search of other records that also might reflect entries to and exits from the White House Complex. No other responsive records were found. See Second Morrissey Decl. ¶¶ 5-6; Ulmer Decl. ¶ 5.

The FOIA requires reasonableness, not perfection or omniscience. See, e.g., Grand Cent. P'ship, Inc. v. Cuomo, 166 F.3d 473, 489 (2d Cir. 1999) (explaining that "an agency's search need not be perfect, but rather need only be reasonable"). Defendant's diligent and thoughtful efforts to discover responsive records demonstrate its commitment to the FOIA and that statute's

[4] Indeed, given the wording of plaintiff's FOIA request, it is questionable whether the Sensitive Security Records are even responsive. See FOIA request at 1; Second Morrissey Decl. ¶ 4.

animating purpose of open government. Its efforts to identify and search for additional records that might prove responsive serve only to enhance the integrity of defendant's search. See Meeropol, 790 F.2d at 953. Based on our prior submissions as supplemented here, the Court should find that defendant has discharged its obligation to conduct a reasonable search.

II. The Sensitive Security Records Are Categorically Exempt From Disclosure Under the FOIA

The Court should hold that the Sensitive Security Records are categorically exempt from disclosure pursuant to FOIA exemptions 2, 7(E), and 7(F) (5 U.S.C. §§ 552(b)(2), (b)(7)(E), and (b)(7)(F)): Revealing these records would undermine the Secret Service's ability to carry out its protective duties.[5] See Ulmer Decl. ¶¶ 17-20.

To reiterate, defendant addresses these records categorically because it cannot confirm or deny the existence of responsive records without compromising its ability to carry out its protective function. Second Morrissey Decl. ¶ 4; Ulmer Decl. ¶¶ 12, 19. Releasing the name of an individual whose visit did or did not prompt the additional protective activities reflected in the Sensitive Security Records would provide insight into the circumstances in which such records are (or are not) created. Second Morrissey Decl. ¶ 4; Ulmer Decl. ¶¶ 12, 19. This information

[5] The Joint Stipulation does not prevent defendant from invoking these exemptions. The Joint Stipulation states that defendant will produce responsive documents "without redactions or claims of exemption." Joint Stipulation ¶ 2. The Joint Stipulation does not cover defendant's claims of exemptions because defendant has not acknowledged the existence of responsive Sensitive Security Records and defendant did not intend for this contract-like document to cover Sensitive Security Records. In any case, public policy concerns, including the protection of the President, Vice President, and White House Complex, suggest that the Joint Stipulation should be interpreted narrowly so as not to cover Sensitive Security Records. See U.S. News & World Report v. Department of the Treasury, Civil Action No. 84-2303, 1986 U.S. Dist. LEXIS 27634, at *6-7 (D.D.C. Mar. 26, 1986) (explaining that "it is difficult to imagine agency procedures or techniques more deserving of protection" than those employed by the Secret Service in its protective capacity).

could allow persons so inclined to figure out the nature of the protective activities reflected in these records. See Brunetti v. FBI, 357 F. Supp. 2d 97, 104 & n.4 (D.D.C. 2004); Second Morrissey Decl. ¶ 4; Ulmer Decl. ¶¶ 12, 19. Of course, a refusal to either confirm or deny the existence of responsive records is a well-recognized and accepted response in circumstances such as these. See, e.g., Phillippi v. CIA, 546 F.2d 1009 (D.C. Cir. 1976) (approving the CIA's refusal to confirm or deny the existence of records related to an underwater sea craft known as the "Glomar Explorer").

A. The Sensitive Security Records Are Categorically Protected by FOIA Exemption 2

Exemption 2 of the FOIA applies to "matters that are . . . related solely to the internal personnel rules and practices of an agency." 5 U.S.C. § 552(b)(2). This exemption applies not only to "trivial administrative matters of no genuine public interest" such as internal file numbers and employee leave policies — referred to as "low 2" records — see Long v. U.S. Dep't of Justice, 450 F. Supp. 2d 42, 54-57 & n.16 (D.D.C. 2006), but also, in some circumstances, to more substantive records "designed to establish rules and practices for agency personnel," known as "high 2" records. Crooker v. Bureau of Alcohol, Tobacco & Firearms, 670 F.2d 1051, 1073 (D.C. Cir. 1981) (en banc).[6] Specifically, "high 2" records are exempt from disclosure if they are "predominantly internal" and their disclosure would "significantly risk[ ] circumvention of agency regulations or statutes." Wiesenfelder v. Riley, 959 F. Supp. 532, 535 (D.D.C. 1997) (quoting Crooker, 670 F.2d at 1074).

[6] The exemption for "low 2" information would justify defendant withholding other information contained in Sensitive Security Records. Ulmer Decl. ¶ 18.

The effect of a record need not be limited to agency personnel for the record to be considered "predominantly internal." In the law enforcement context, for example, "agency guidelines for conducting investigations and identifying law violators" are treated as "predominantly internal" even though they "directly affect[ ] the public at large." Wiesenfelder, 959 F. Supp. at 535; cf. Institute for Policy Studies v. Department of the Air Force, 676 F. Supp. 3, 5 (D.D.C. 1987) (acknowledging that Exemption 2 applies to "law enforcement records," among other types). The D.C. Circuit has held, for example, that Exemption 2 covers an ATF training manual regarding surveillance of suspects, finding that the manual was "predominantly internal" because its purpose was not "to modify or regulate public behavior [but] only to observe it for illegal activity." Crooker, 670 F.2d at 1076. Similarly, another judge of this Court has held that Exemption 2 covers "trigger figures" and "error rates" used by the Department of Education to determine when an educational institution may not be in compliance with federal guidelines in student financial aid programs. See Wiesenfelder, 959 F. Supp. at 534-36. The Court rejected a contention that these benchmarks constituted "secret law" governing the agency's "dealings with the public." Id. at 536. Public behavior, the Court observed, was governed by the statute; the trigger figures and error rates, in contrast, were used internally to "alert the Department . . . for enforcement purposes" and to enable the Department "to most closely scrutinize the institutions exhibiting the most serious violations." Id. at 536-37.

Nor is Exemption 2 limited to the actual text of agency "rules or practices." Rather, as stated in the statutory language, it extends to matters "related" to internal rules and practices. Thus, as the D.C. Circuit has held, Exemption 2 protects records whose "disclosure could lead to disclosure of the rule or practice itself." Schwaner v. Department of Air Force, 898 F.2d 793,

796 (D.C. Cir. 1990) (emphasis added). Thus, for example, another judge of this Court has held that Exemption 2 covers informant numbers and file numbers used in FBI records to protect the identity of informants. See Brunetti v. FBI, 357 F. Supp. 2d 97, 104 & n.4 (D.D.C. 2004). Although disclosure of the numbers, alone, would not reveal informant identities, the Court noted that their disclosure could lead to that result:

> Because these unique identifiers are used consistently across FBI records, it would be possible, with access to the numbers, to discern patterns of information associated with particular sources. An individual with knowledge of the people and facts would be able to deduce the identities of these sources, putting the sources at risk of exposure and potentially placing them in danger. Accordingly, the Court concludes that the release of the numbers would risk revealing the identities of informants in circumvention of FBI policies and practices related to information gathering and protecting confidential informants.

Id.

The requirement that disclosure of a "high 2" record would "significantly risk[ ] circumvention of agency regulations or statutes" is met where disclosure would endanger the safety of agency personnel or of persons under their protection. For example, a judge of this Court has held that Exemption 2 protects an "internal investigation document used by the Secret Service to analyze and profile factual information concerning individuals" who are "potential threat[s] toward a Secret Service protectee." Dorsett, 307 F. Supp. 2d at 36. "As such," said the Court, "the documents could be used to gain insight into the methods and criteria the Secret Service utilizes to identify and investigate persons of interest, and could alter such individuals' behavior to avoid detection" — thus presenting a "significant risk" of circumvention of statutes. Id. Similarly, another judge has held that the exemption applies to guidelines used by an agency security office in protecting the head of the agency, where disclosure would increase the potential

for "unlawful attacks." Judicial Watch, Inc. v. U.S. Dep't of Commerce, 337 F. Supp. 2d 146, 166 (D.D.C. 2004).

Under this precedent, the Sensitive Security Records involved here fall squarely within the protection of Exemption 2. Like the Department of Education "trigger figures" and "error rates" at issue in Wiesenfelder, these records are designed to "alert" defendant to potential security threats and to "most closely scrutinize" those White House Complex visitors and visits that might present "the most serious" risk. See Wiesenfelder, 959 F. Supp. at 536-37; Ulmer Decl. ¶¶ 17, 19. Although disclosing the names of persons whose visits have prompted defendant to undertake additional security activities would not, alone, expose the nature of defendants protective activities, revealing that information could allow someone "with knowledge of the people and facts" to "deduce" the nature of those additional protective activities. Brunetti, 357 F. Supp. 2d at 104; see Ulmer Decl. ¶¶ 17, 19. Like the records held properly exempt in Brunetti, therefore, disclosing defendant's Sensitive Security Records could "lead to" disclosure of certain aspects of the agency's fulfillment of its protective functions. See Brunetti, 357 F. Supp. 2d at 104; Ulmer Decl. ¶¶ 17, 19; Schwaner, 898 F.2d at 796. Finally, like the records withheld in Dorsett, the records in question here "could be used to gain insight into the methods and criteria the Secret Service utilizes" to secure the White House and its protectees; disclosure, therefore, would "significantly risk[ ] circumvention" of statutes. 307 F. Supp. 2d at 36; Ulmer Decl. ¶ 17, 19.

B. The Sensitive Security Records Are Categorically Protected by FOIA Exemption 7(E)

"Exemption 7(E) provides categorical protection to information related to law enforcement techniques." Smith v. Bureau of Alcohol, Tobacco and Firearms, 977 F. Supp. 496, 501 (D.D.C. 1997). Records "compiled for law enforcement purposes" may be withheld under this exemption if release of the information "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E). The D.C. Circuit applies a "deferential standard to a claim that information was compiled for law enforcement purposes when the claim is made by an agency whose primary function involves law enforcement." Tax Analysts v. IRS, 294 F.3d 71, 77 (D.C. Cir. 2002); see Blanton v. U.S. Dep't of Justice, 63 F. Supp. 2d 35, 44 (D.D.C. 1999) ("Law enforcement agencies . . . face a lesser burden with regard to showing a legitimate law enforcement purpose behind the compilation of such records than do other agencies."). Specifically, in order to show that information was "compiled for law enforcement purposes," a law enforcement agency must show that (1) the activity that gave rise to the documents is related to the enforcement of federal laws or the maintenance of national security; and (2) the nexus between the activity and one of the agency's law enforcement duties is based on information sufficient to support at least a "colorable claim" of its rationality. See Pratt v. Webster, 673 F.2d 408, 420-21 (D.C. Cir. 1982); Blanton, 63 F. Supp. 2d at 44. Thus, "a court can accept less exacting proof from [a law enforcement] agency that the purpose underlying disputed documents is law enforcement." See Tax Analysts, 294 F.3d at 77.

In examining an Exemption 7 claim, the courts are sensitive to the inherent limitations on describing the purposes of law enforcement records, given that such a description may itself disclose law enforcement techniques and procedures. Therefore, "[i]n justifying the application of Exemption 7(E), the agency may describe the general nature of the technique while withholding the full details." Boyd v. Bureau of Alcohol, Tobacco, Firearms, and Explosives, Civil Action No. 05-1096 (RMU), 2006 WL 2844912, at *9 (D.D.C. Sept. 29, 2006). In fact, "in some cases it may not even be possible for an agency to describe its law enforcement techniques in general terms without disclosing the very information it seeks to protect." Morley v. CIA, 453 F. Supp. 2d 137, 156 (D.D.C. 2006).

Under these standards, any Sensitive Security Records that would be withheld by defendant in this case would be protected by Exemption 7(E). See Ulmer Decl. ¶¶ 17, 19. As a threshold matter, defendant's protective function constitutes "law enforcement" for purposes of Exemption 7. See 18 U.S.C. § 3056A(a) (referring to Secret Service Uniformed Division as a "permanent police force"). As another judge of this Court has said, in holding that defendant's protective function is a "law enforcement" activity under Exemption 7:

> The Secret Service is unique in that its law enforcement efforts are geared primarily towards prevention rather than apprehension. . . . While most law enforcement agencies investigate suspected or on-going criminal activities, the Secret Service must protect persons such as the President from both known and unknown threats. Accordingly, many of its most important techniques and procedures are preventative rather than investigative. It is inconceivable, however, that Congress meant to afford these activities any less protection from disclosure simply because they do not fit within the traditional notion of investigative law enforcement techniques. Indeed, it is difficult to imagine agency procedures or techniques more deserving of protection.

U.S. News & World Report, 1986 U.S. Dist. LEXIS 27634, at *6-7; see Moorefield v. U.S. Secret Service, 611 F.2d 1021, 1024 (5th Cir. 1980) (holding that Secret Service records were "compiled for law enforcement purposes" where they "were prepared to help the Service fulfill its duty under 18 U.S.C. § 3056 (1976) [of] ensuring the lives and safety of the President, members of his family, and certain other persons"); see also Dorsett v. U.S. Dep't of the Treasury, 307 F. Supp. 2d 28, 38-40 (D.D.C. 2004) (upholding Secret Service's invocation of Exemption 7(C)); Fitzgibbon v. U.S. Secret Service, 747 F. Supp. 51, 59 (D.D.C. 1990) (upholding Secret Service's invocation of Exemptions 7(C) and (D)).

Obviously, therefore, the Sensitive Security Records are "compiled for law enforcement purposes." 5 U.S.C. § 552(b)(7)(E); Ulmer Decl. ¶ 10; Second Morrissey Decl. ¶ 3. They are created and used in the course of conducting background checks and other security-related activities regarding certain visitors to the White House Complex, in furtherance of defendant's statutory duties. See Ulmer Decl. ¶ 10; Second Morrissey Decl. ¶ 3; see also Pratt, 673 F.2d at 420-21; Blanton, 63 F. Supp. 2d at 44. Like the records involved in Moorefield, cited above, these records were "prepared to help the Service fulfill its [protective] dut[ies]." 611 F.2d at 1024; see 18 U.S.C. §§ 3056, 3056A.

Furthermore, disclosing these records "would disclose techniques and procedures" used by defendant in carrying out these duties. 5 U.S.C. § 552(b)(7)(E). As explained by defendant, these records are created in conducting additional background checks and other security-related activities regarding certain visitors who are chosen based on certain details in their backgrounds and/or the circumstances of their visits. See Ulmer Decl. ¶ 10; Second Morrissey Decl. ¶ 3. Disclosing these records could, among other things, reveal the criteria — not generally known to

the public — that defendant uses in choosing visitors for these additional background checks and other security-related activities. See Ulmer Decl. ¶¶ 17, 19.

Under these circumstances, the Sensitive Security Records are categorically protected from disclosure by FOIA Exemption 7(E).

C. The Sensitive Security Records Are Categorically Protected by FOIA Exemption 7(F)

Exemption 7(F) of the FOIA exempts from disclosure "records or information compiled for law enforcement purposes," the disclosure of which "could reasonably be expected to endanger the life or physical safety of any individual." 5 U.S.C. § 552(b)(7)(F). "While courts generally have applied Exemption 7(F) to protect law enforcement personnel or other specified third parties, by its terms, the exemption is not so limited; it may be invoked to protect 'any individual' reasonably at risk of harm." Long v. U.S. Dep't of Justice, 450 F. Supp. 2d 42, 79 (D.D.C. 2006). "In evaluating the validity of an agency's invocation of Exemption 7(F), the court should within limits, defer to the agency's assessment of danger." Peter S. Herrick's Customs & Inter'l Trade Newsletter v. U.S. Customs & Border Protection, Civil Action No. 04-00377 (JDB), 2006 WL 1826185, at *9 (D.D.C. June 30, 2006) (internal quotation marks omitted). This exemption "does not require a balancing of interests, but rather focuses on the potential harm to the third party." Brunetti v. FBI, 357 F. Supp. 2d 97, 109 n.9 (D.D.C. 2004).

Defendant's factual submissions in this case establish that the Sensitive Security Records are categorically protected by Exemption 7(F). Ulmer Decl. ¶ 20. As discussed above in relation to Exemption 7(E), disclosure of these records would reveal certain "techniques and procedures" used by defendant in securing the White House Complex, by revealing when various security

checks and security measures are taken in connection with individuals seeking entrance into the Complex. Id. Disclosing those techniques and procedures would permit an individual or organization to attempt to avoid certain security checks, potentially impeding defendant's efforts to identify persons who may be a threat to its protectees. Id. Since the function of defendant includes the protection of particular personnel, disclosing these records "could reasonably be expected to endanger the life or physical safety" of one or more Secret Service protectees.[7] 5 U.S.C. § 552(b)(7)(F); see Ulmer Decl. ¶ 20.

CONCLUSION

For the reasons stated above, the Court should enter summary judgment in favor of defendant.

Dated: November 30, 2007

Respectfully submitted,

JEFFREY S. BUCHOLTZ
Acting Assistant Attorney General

---

[7] The law not only supports defendants' argument that any responsive Sensitive Security Records would be exempt from the FOIA pursuant to Exemptions 2, 7(E), and 7(F), but it also would justify defendant in withholding the following information under Exemptions 6 and 7(C): the names of the individuals requesting that visitors be given access to the Complex and the Social Security numbers and dates of birth of the individuals for whom access is sought. See Ulmer Decl. ¶¶ 21-25. Birth dates and Social Security numbers are typical of the sensitive personal information whose disclosure would "constitute a clearly unwarranted invasion of personal privacy," see 5 U.S.C. § 552(b)(6), (b)(7)(C), and plaintiff can show no legitimate interest in their disclosure here. See, e.g., Judicial Watch, Inc. v. U.S. Dep't of Commerce, 337 F. Supp. 2d 146 (D.D.C. 2004) ("[T]he disclosure of [dates of birth and other personal] information has little to do with the public's understanding of the manner in which the DOC conducts business."); Hertzberg v. Veneman, 273 F. Supp. 2d 67, 86 n.13 (D.D.C. 2003) ("The Court agrees with defendant . . . that there is a significant privacy interest in social security numbers, and no legitimate purpose would be served by their release."); Kuffel v. U.S. Bureau of Prisons, 882 F. Supp. 1116, 1122-23 (D.D.C. 1995) (upholding exemption of "the social security numbers of Plaintiff's prospective visitors in prison").

JEFFREY A. TAYLOR
United States Attorney

CARL J. NICHOLS
Deputy Assistant Attorney General

JOSEPH H. HUNT
Branch Director

ELIZABETH J. SHAPIRO
Assistant Branch Director

OF COUNSEL:

LIZA MURPHY
MOLLY WEBER
United States Secret Service

s/ Justin M. Sandberg
JUSTIN M. SANDBERG
(Ill. Bar. No. 6278377)
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W. #7224
P.O. Box 883 Ben Franklin Station
Washington, D.C. 20044
Telephone: (202) 514-3489
Facsimile: (202) 616-8202
E-mail: justin.sandberg@usdoj.gov

Attorneys for Defendant

EXHIBIT 1

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

JUDICIAL WATCH,	)	
	)	
Plaintiff,	)	
	)	CIVIL ACTION NO.
v.	)	06-310 (RMC)
	)	
UNITED STATES SECRET SERVICE,	)	
	)	
Defendant.	)	
	)	

SECOND DECLARATION OF PAUL S. MORRISSEY
DEPUTY ASSISTANT DIRECTOR
OFFICE OF PROTECTIVE OPERATIONS
UNITED STATES SECRET SERVICE

I, Paul S. Morrissey, hereby declare as follows:

1. I am the Deputy Assistant Director of the Office of Protective Operations ("OPO") for the United States Secret Service ("Secret Service"), which is a component of the Department of Homeland Security ("DHS"). I have held this position since September 2006, and have been employed with the Secret Service as a Special Agent (GS-1811) since January 1983.

2. This declaration supplements my December 12, 2006, declaration regarding the search for records responsive to Judicial Watch's January 20, 2006, Freedom of Information Act ("FOIA") request. The statements made herein are based on my personal knowledge or on information made available to me in my official capacity since that declaration.

3. Beyond Secret Service Form (SSF) 1888s and related paper records (described in my December 12, 2006 declaration), the Secret Service sometimes creates other records that relate to the background investigation and security process conducted in connection with certain individuals entering or scheduled to enter the White House Complex (referred to herein as

"Sensitive Security Records"). These records are created in the course of conducting additional background checks and other security-related activities regarding certain visitors, who are chosen by the Secret Service based on certain details in their backgrounds and/or the circumstances of their visits. The records include the names and other identifying information concerning such visitors (including, in some cases, their birth dates and/or Social Security numbers) and background information on them or information regarding their visits to the Complex, which may include criminal history and/or other security-related information. The persons whose visits to the White House are reflected in these records should also be reflected in the Worker and Visitor Entrance System ("WAVES") records.

4. The focus of the searches for records responsive to Judicial Watch's request described in the first and second declarations of Kathy J. Lyerly submitted in this case was on the WAVES and Access Control Records System ("ACR") data/records. Although it is not clear that the Sensitive Security Records are responsive to the request, the Secret Service now believes that they could be potentially responsive. The Secret Service is, however, concerned that if the Secret Service were to reveal to the plaintiff whether there were, or were not, any Sensitive Security Records concerning the specific individual at issue in plaintiff's FOIA request, that fact, combined with other such information repeated over time, could lead to the gathering of information concerning whether and when such additional security checks are conducted. This possibility constitutes a security risk.

5. Leaving aside the Sensitive Security Records, the Secret Service has conducted additional searches in certain categories of records for the name of the individual listed in the subject FOIA request: records originating from the Executive Office of the President reflecting

parking requests, or authorization for parking, with respect to the White House Complex; electronically maintained e-mails at the WAVES Center requesting access to the White House Complex; and White House Daily Briefing Sheets. These searches included the period of January 1, 2001 through July 6, 2006 (although it is believed that not all records that were created during this period still exist), and were conducted only after they were authorized by the Office of the President and the Office of the Vice President. Again, it is questionable whether these categories are even responsive to Judicial Watch's request. In any case, however, no responsive records were found in any of these groups.

6. The Secret Service has also conducted a search for the name "Jack Abramoff" in the WAVES and ACR records on the June and July 2006 CD-ROMs (to search for responsive records through July 6, 2006). No responsive records were found. I am advised that these additional WAVES and ACR records were searched because of the belief that the previous searches encompassed only records downloaded from the server as of the dates of these searches.

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

Executed on November 30th, 2007.

PAUL S. MORRISSEY

EXHIBIT 2

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

JUDICIAL WATCH,	)	
	)	
Plaintiff,	)	
	)	CIVIL ACTION NO.
v.	)	06-310 (RMC)
	)	
UNITED STATES SECRET SERVICE,	)	
	)	
Defendant.	)	
	)	

DECLARATION OF CRAIG W. ULMER
SPECIAL AGENT IN CHARGE
FREEDOM OF INFORMATION AND PRIVACY ACTS OFFICER
UNITED STATES SECRET SERVICE

I, Craig W. Ulmer, hereby declare as follows:

1. I am the Special Agent in Charge, Freedom of Information and Privacy Acts (FOI/PA) Officer for the United States Secret Service (hereinafter "Secret Service"), which is a component of the Department of Homeland Security ("DHS"). I have been the Secret Service FOI/PA Officer since August 5, 2007. I have been employed with the Secret Service as a Special Agent (GS-1811) since April 28, 1985.

2. DHS regulations, Title 6, Code of Federal Regulations, section 5.4, and Appendix A, II(I)(3), vest authority in the FOI/PA Officer, Secret Service, to make initial determinations as to whether to grant Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, requests for Secret Service records (68 FR 4056, 4058, and 4069).

3. The statements made in this declaration are based on information made available to me in my official capacity.

4. As the Secret Service's FOI/PA Officer, I am familiar with plaintiff's FOIA request

to the Secret Service.

5. Pursuant to search requests from myself (or my office), the Secret Service has conducted additional searches in certain record groups for documents/records responsive to plaintiff's FOIA request: records originating from the Executive Office of the President reflecting parking requests, or authorization for parking, with respect to the White House Complex; White House Daily Briefing Sheets; Worker and Visitor Entrance System ("WAVES") and Access Control Records System ("ACR") records on the June and July 2006 CD-ROMs; and, electronically maintained e-mails at the WAVES Center requesting access to the White House Complex. Those searches, which I have been advised were conducted only after they were authorized by the Office of the Vice President and/or the Office of the President, have now been completed, and no records responsive to plaintiff's FOIA request were located.

6. With respect to an additional record group, defined below as "Sensitive Security Records," the Secret Service cannot confirm or deny whether any responsive records exist. To do so would reveal whether the individual named in plaintiff's FOIA request had been subject to certain additional security check(s). Such information, if combined with other information, could reveal when certain additional background checks are, or are not, conducted by the Secret Service. Revealing such information would, therefore, present a security risk.

7. To the extent that any responsive records exist, the information contained in the records is exempt pursuant to FOIA exemptions codified at 5 U.S.C. §§ 552(b)(2), (b)(6), (b)(7)(C), (b)(7)(E), and (b)(7)(F). A description and explanation of the application of these exemptions to Sensitive Security Records is set forth below.

Plaintiff's FOIA Request

8. By letter dated January 20, 2006, and received by the Secret Service FOI/PA Office on January 23, 2006, plaintiff submitted to the Secret Service a FOIA request for:

> any and all agency records concerning, relating to, or reflecting the following subjects: All White House visitor logs from January 1, 2001 to present that reflect the entries and exit(s) of lobbyist Jack Abramoff from the White House.

Previous Releases

9. I have been advised that in connection with prior searches, WAVES data and ACR data/records regarding the individual named in plaintiff's FOIA request were released to the plaintiff in this case.

Sensitive Security Records

10. In connection with its statutory responsibilities as set forth in Title 18 of the United States Code, sections 3056 and 3056A, the Secret Service sometimes creates records that relate to the background investigation and security process conducted in connection with certain individuals entering or scheduled to enter the White House Complex (hereinafter referred to as "Sensitive Security Records"). These records are created in the course of conducting additional background checks and other security-related activities regarding certain visitors, who are chosen by the Secret Service based on certain details in their backgrounds and/or the circumstances of their visits. The persons whose visits to the White House are reflected in the Sensitive Security Records should also be reflected in WAVES records.

11. In the course of litigating another case with a similar FOIA request, the Office of Protective Operations ("OPO") discovered that an electronic table was being populated that contains certain Sensitive Security Records that date back to March 2003. OPO also has paper

records that constitute Sensitive Security Records; however, those paper records only date back to October 2006. The Office of the Assistant Director, Office of Protective Research ("OPR"), Intelligence Division, also has paper records that constitute Sensitive Security Records, but those too only date back to October 2006, with some sporadic records dating back to September 2006.

12. Because revealing whether responsive records exist in this case would allow individuals to piece together the circumstances under which the additional checks are done, the Secret Service cannot confirm or deny the existence of responsive records.

FOIA Exemptions Claimed

13. Even if potentially responsive Sensitive Security records were located, however, this information would be subject to FOIA exemptions.

14. Information in the Sensitive Security Records could include the following: the name of an internal Secret Service security program; the name of the individual who made the request for the appointment; appointment date and time; the time and date a report was run; a number letter sequence associated with an Access Control Officer who requested the report; the date and time of the request for the appointment; an appointment letter and number sequence assigned to an appointment for access to the White House Complex by a computer system; information concerning who the appointment is with; the name, Social Security number, date of birth, city and state of residence for the individual seeking access to the White House Complex for whom the security check is being requested; and information confirming certain background checks to be conducted.

15. Any and all potentially responsive information in the Sensitive Security Records would have been compiled for law enforcement purposes. All of the information would have

been gathered and utilized by the Secret Service in connection with its statutory responsibilities for protection and security, as set forth in Title 18 of the United States Code, sections 3056 and 3056A. Therefore, all of the potentially responsive information would meet the threshold requirement for exemption from release under the provisions of the FOIA, section 552(b)(7).

16. Any potentially responsive information in the Sensitive Security Records would be withheld from release in its entirety under the FOIA, sections 552(b)(2), (b)(6), (b)(7)(C), (b)(7)(E), and (b)(7)(F). A detailed discussion of the basis for invoking these exemptions set forth in the following paragraphs.

FOIA Exemptions (b)(2) and (b)(7)(E)

17. To the extent that potentially responsive information could be located in a search of the Sensitive Security Records in connection with plaintiff's FOIA request, this information would be withheld under Title 5 of the United States Code, section 552(b)(2), and in some cases under 552(b)(2) in conjunction with section 552(b)(7)(E). Section 552(b)(2) exempts from disclosure information "relating solely to the internal personnel rules and practices of an agency." Section 552(b)(7)(E) 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. . .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."

18. Such potentially responsive information that would be withheld under exemption (b)(2) includes the appointment letter/number sequence assigned to an appointment by the computer; and a letter/number sequence associated with an Access Control Officer. These pieces

of information relate strictly to the internal operation of the system and provide no information to the public. Therefore, this information would be withheld under a low (b)(2) exemption.

19. Any and all potentially responsive information in Sensitive Security Records would have been compiled for law enforcement purposes, and in connection with the Secret Service's protective responsibilities as set forth under Title 18 of the United States Code, sections 3056 and 3056A. To release the information could disclose information related to when and if various security checks and security measures are taken in connection with individuals seeking entrance into the White House Complex. For instance, the abbreviated name of the program as shown on a potentially responsive document itself could reveal security-related information concerning when certain checks are, or are not, conducted. Further, to reveal the name of and personal identifying information concerning the individual, and who he was visiting, could suggest when additional security checks are conducted and when certain security measures are not, or are unlikely, to be taken. Thus, the name, personal identifying information, and intended visitee information must also be withheld as such details may indicate certain security related activity, or the lack thereof. Further, in this case, as the plaintiff's FOIA request seeks information concerning only one individual, if the Secret Service were to search for any such record and then release the fact of whether this search had or had not located any such responsive records, that release of information in and of itself, could, when repeatedly combined with other information, reveal when such security checks are or are not conducted. Release of the information would reveal information not known to the general public. Further, the release of the information would reveal techniques and criteria used by the Secret Service to gather additional information in certain circumstances and in regard to certain individuals. Disclosing any potentially responsive

information (including whether a search for a particular individual's name located, or did not locate a record), could, when repeatedly combined with other similar information, reasonably be expected to enable individuals to circumvent the law by revealing information regarding the circumstances that trigger when certain security steps are taken, and the manner through which those additional security checks are taken or information is gathered. For this reason, any and all such potentially responsive information located in connection with plaintiff's FOIA request would be withheld under a high (b)(2) exemption in conjunction with exemption (b)(7)(E).

FOIA Exemption (b)(7)(F)

20. Title 5, United States Code, section 552(b)(7)(F), exempts from disclosure "records or information compiled for law enforcement purposes," the disclosure of which "could reasonably be expected to endanger the life or physical safety of any individual." As discussed above, release of any potentially responsive Sensitive Security Records could disclose information related to when and if various security checks and security measures are taken in connection with individuals seeking entrance into the White House Complex. One purpose of those security checks and security measures is to protect the life and physical safety of one or more protectees of the Secret Service. Disclosing the Secret Service's techniques and procedures in that regard could permit an individual or organization to attempt to avoid certain security checks, potentially impeding the Secret Service's efforts to identify persons who may be a threat to its protectees, and thus potentially endangering the life and physical safety of one or more Secret Service protectees.

FOIA Exemptions (b)(6) and (b)(7)(C)

21. Title 5, United States Code, section 552(b)(6), exempts from disclosure

information about individuals in "personnel and medical files" when the disclosure of such information "would constitute a clearly unwarranted invasion of personal privacy." 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."

22. Exemptions (b)(6) and (b)(7)(C) would be cited to justify redacting, from Sensitive Security Records, the name of the individual making the request for access and the Social Security number and date of birth for the individual seeking access to the White House Complex.

23. In making its determination that it would withhold this information under exemptions (b)(6) and (b)(7)(C), the Secret Service would balance the public's interest in disclosure against the rights to personal privacy of the individual named, and determine that the privacy rights of the individual outweigh any public interest in disclosure.

24. First, in regard to the name of the individual making the access request, there would appear to be little public interest in such information. Yet, the release of such information could invade the individual's privacy by causing him/her public attention or subjecting the individual to unnecessary and unwanted contact. Therefore, any such information would be withheld under exemptions (b)(6) and (b)(7)(C).

25. Second, though the individual about whom plaintiff seeks information has received substantial notoriety, the Secret Service would withhold his Social Security number and date of birth under exemptions (b)(6) and (b)(7)(C). Such information, combined with the individual's name, could lead to various forms of criminal activity against the named individual, such as identity theft or fraud. Even in the case of an individual who has received the notoriety

surrounding the individual named by the plaintiff's FOIA, there seems to be no reason why the combination of that person's Social Security number and date of birth should flow into the public domain, or why the public would have a valid interest in such identifying information. Considering these factors, the date of birth and Social Security number of this individual would be withheld under exemptions (b)(6) and (b)(7)(C).

Segrebility of Information

26. Based on the information that would be withheld in a potentially responsive Sensitive Security Record, it would not be possible to segregate any responsive information, because the remaining information on a document would be meaningless. Once information such as the name of a program; the name, Social Security number, date of birth, and other identifying information concerning the individual subject to the security process; and information that indicates when and by whom the process is triggered is removed, the remaining information would be a blank form. Therefore, there would be no information that could be reasonably segregated and released to plaintiff. Also, of course, releasing any information would reveal the existence of a responsive record, thereby creating a security risk.

Conclusion

27. In completing its protective and investigative functions, the Secret Service must protect from disclosure identifying information regarding third parties, and must protect the integrity of its security and protection related processes and information. For these reasons, the Secret Service cannot confirm or deny the existence of potentially responsive information in connection with plaintiff's FOIA request with respect to the Sensitive Security Records; but asserts that if such responsive information existed, it would be withheld in full.

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

NOVEMBER 30, 2007
Date

Craig W. Ulmer
Craig W. Ulmer
SAIC, FOIA/PA Officer

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

JUDICIAL WATCH INC.,	
Plaintiff,	
v.	
UNITED STATES SECRET SERVICE,	Civil Action No. 06-310 (RMC)
Defendant.	

PROPOSED ORDER

UPON CONSIDERATION of Defendant's Supplemental Motion for Summary Judgment, any Opposition thereto, and the whole record herein, it is hereby, this ____ day of _____, 2007

ORDERED that defendant's motion is granted, and it is

FURTHER ORDERED that this action be, and hereby is, dismissed.

_____
UNITED STATES DISTRICT JUDGE