UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

CHRISTOPHER EARL STRUNK,

Plaintiff,

v.

UNITED STATES DEPARTMENT OF STATE, *et al.*,

Defendants.

Civil Action No. 08-2234 (RJL)

MEMORANDUM OPINION

(November 20 2012) [Dkt. #58]

This matter is before the Court on Defendant's Renewed Motion for Summary Judgment [Dkt. #58]. For the reasons discussed below, the motion is GRANTED.

BACKGROUND

Plaintiff brought this action under the Freedom of Information Act ("FOIA"), *see* 5 U.S.C. § 552, in order to obtain information about President Barack Obama and his late mother, Stanley Ann Dunham, from the United States Department of State ("State Department") and United States Customs and Border Protection ("CBP"), a component of the United States Department of Homeland Security ("DHS"). With respect to plaintiff's request for information about President Obama, the Court has ruled that plaintiff failed to submit proper FOIA requests to the State Department and DHS because neither request included a written authorization from President Obama for the release of information to plaintiff. *Strunk v. U.S. Dep't of State*, 693 F. Supp. 2d 112, 115 (D.D.C. 2010). The Court also has concluded that the State Department and CBP conducted reasonable searches for records responsive to plaintiff's requests for information about Ms. Dunham. *Strunk v. U.S. Dep't of State*, 770 F. Supp. 2d 10, 16 (D.D.C. 2011); *Strunk v. U.S. Dep't of State*, 845 F. Supp. 2d 38, 45 (D.D.C. 2012). Although CBP properly withheld certain information under Exemption 6, *Strunk*, 845 F. Supp. 2d at 45-46, it did not previously demonstrate that it properly withheld other pieces of information under Exemption 7(E), *id.* at 47.

The sole issue remaining for resolution is whether the CBP properly withheld information under Exemption 7(E) from a one-page document described as a "TECS Printout of Travel Documents for Stanley Dunham for Dates January 1, 1982 to December 31, 1985." Vaughn Index, Ex. B to Declaration of Dorothy Pullo ("Second Pullo Decl.") [Dkt. #52-1], Attach. to Mem. of Law in Supp. of Def.'s Mot. for Summ. J., Apr. 29, 2011 [Dkt. #52].[1]

[1] The declarant explained that TECS "began capturing traveler arrivals and departures into and out of the United States beginning in January of 1982," and that paper records in use prior to TECS "no longer exist and are no longer archived." Second Pullo Decl. ¶ 8.

DISCUSSION[2]

I. Summary Judgment in a FOIA Case

"FOIA cases typically and appropriately are decided on motions for summary judgment." *Defenders of Wildlife v. U.S. Border Patrol*, 623 F. Supp. 2d 83, 87 (D.D.C. 2009). The Court will grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and that it is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(a). In a FOIA action to compel production of agency records, the agency "is entitled to summary judgment if no material facts are in dispute and if it demonstrates 'that each document that falls within the class requested either has been produced . . . or is wholly exempt from the [FOIA's] inspection requirements.'" *Students Against Genocide v. Dep't of State*, 257 F.3d 828, 833 (D.C. Cir. 2001) (quoting *Goland v. CIA*, 607 F.2d 339, 352 (D.C. Cir. 1978)).

Summary judgment may be based solely on information provided in an agency's supporting affidavits or declarations if they are relatively detailed and when they describe

[2] The Court has reviewed plaintiff's opposition to the renewed motion for summary judgment, and finds that it utterly fails to address CBP's reliance on Exemption 7(E) in withholding certain information. Ordinarily, the Court may treat as conceded any argument raised in a motion which the opposing party fails to address. *See, e.g.*, *Augustus v. McHugh*, No. 02-cv-2545, 2012 WL 2512930, at *4 (D.D.C. July 2, 2012) (holding that because plaintiff's "opposition did not challenge the Secretary's proffered justifications under FOIA for having redacted [information,]" the arguments were "deemed conceded, and summary judgment [was] entered in favor of the Secretary"); *People for the Ethical Treatment of Animals v. Nat'l Inst. of Health,* 853 F. Supp. 2d 146, 151 (D.D.C. 2012) ("Plaintiff also did not respond to defendant's arguments with respect to Count I or Count III in its opposition to defendant's motion for summary judgment," and, accordingly, "the Court . . . treat[ed] Count I and III as conceded and . . . dismiss[ed] these claims without prejudice"); *see also* LCvR 7(h). In this case, however, the Court will discuss briefly the applicability of Exemption 7(E) to CBP's redactions from the TECS-generated document at issue.

"the documents and the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemption, and are not controverted by either contrary evidence in the record [or] by evidence of agency bad faith." *Military Audit Project v. Casey*, 656 F.2d 724, 738 (D.C. Cir. 1981). "To successfully challenge an agency's showing that it complied with the FOIA, the plaintiff must come forward with 'specific facts' demonstrating that there is a genuine issue with respect to whether the agency has improperly withheld extant agency records." *Span v. U.S. Dep't of Justice*, 696 F. Supp. 2d 113, 119 (D.D.C. 2010) (quoting *U.S. Dep't of Justice v. Tax Analysts,* 492 U.S. 136, 142 (1989)).

II. Law Enforcement Records

Exemption 7 protects from disclosure "records or information compiled for law enforcement purposes," but only to the extent that disclosure of such records would cause an enumerated harm.

> A record is deemed to have been created or compiled for a law enforcement purpose only if (1) it arose from an investigation related to the enforcement of federal laws or to the maintenance of national security (the nexus requirement), and (2) the nexus between the investigation and one of the agency's law enforcement duties is based on information sufficient to support at least a colorable claim of its rationality.

Simon v. Dep't of Justice, 980 F. 2d 782, 783 (D.C. Cir. 1992) (quoting *Pratt v. Webster,* 673 F.2d 408, 420-21 (D.C. Cir. 1982)) (brackets and internal quotation marks omitted). A law enforcement agency's "decision to invoke [E]xemption 7 is entitled to deference," *Campbell v. U.S. Dep't of Justice*, 164 F.3d 20, 32 (D.C. Cir. 1998) (citing *Pratt*, 673

F.2d at 419), but deference does not amount to blind acceptance of the agency's assertions, *see Lardner v. Dep't of Justice*, 638 F. Supp. 2d 14, 32 (D.D.C. 2009) (citing *Campbell*, 164 F.3d at 32) ("The D.C. Circuit has made clear. . . that an agency's broad claim that its files are law enforcement files—without addressing the particular documents at issue—is insufficient to establish that the specific documents in dispute within those files are law enforcement records under FOIA."), *aff'd*, 398 F. App'x 609 (D.C. Cir. 2010) (per curiam).

CBP's declarant states that the agency is "a law enforcement agency with enforcement responsibilities for over 400 Federal statutes, on behalf of over 20 different federal agencies." Second Pullo Decl. ¶ 21. Its principal functions include the protection of the United States' borders "against terrorists and the instruments of terror," enforcement of customs and immigration laws, facilitation of "lawful international trade and travel [and] the processing of passengers, conveyances, and merchandise entering, transiting and departing the United States." *Id.*

TECS is described as "an overarching law enforcement information, collection, analysis, and sharing environment that securely links telecommunications devices and personal computers to a central system and database." *Id.* ¶ 7. Its "several modules [are] designed to collect, maintain, and screen data as well as conduct analysis, screening, and information sharing." *Id.* Its databases "contain temporary and permanent enforcement, inspection and intelligence records relevant to the anti-terrorism and law enforcement mission of CBP and numerous other federal agencies that it supports," and it is a means for "direct access to other major law enforcement systems, including the Department of

Justice's National Crime Information Center (NCIC), the National Law Enforcement Telecommunications System (NLETS), and the Canadian Police Information Centre (CPIC)." *Id.* Further, "TECS maintains limited information on those individuals who have been granted access to the system." *Id.*

"Border Crossing Information (BCI) is a subset of data connected to TECS. BCI receives and maintains border crossing information on travelers who are admitted . . . into the United States," such as biographical information, photographs, itinerary information provided by air and sea carriers, and the time and location of the border crossing. *Id.* ¶ 8. CBP operates and uses TECS "to conduct enforcement checks on individuals seeking to enter or depart the United States." *Id.* ¶ 7. Information responsive to plaintiff's FOIA request "for travel documents related to Stanley Ann Dunham," *id.* ¶ 5, is maintained in TECS and TECS is "the only place to search for arrival and departure records" of a particular individual, *id.* ¶ 9. CBP thus establishes that the relevant records were compiled for a law enforcement purpose.

III. Exemption 7(E)

Exemption 7(E) protects from disclosure law enforcement records "to the extent that the production of such . . . 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 first clause of Exemption 7(E) affords 'categorical' protection for 'techniques and procedures' used in law enforcement investigations or prosecutions." *Pub. Emps. for Envtl. Responsibility v.*

U.S. Section Int'l Boundary & Water Comm'n, U.S. - Mexico, 839 F. Supp. 2d 304, 327 (D.D.C. 2012) (citing *Showing Animals Respect & Kindness v. U.S. Dep't of the Interior*, 730 F. Supp. 2d 180, 199-200 (D.D.C. 2010)). "Exemption 7(E)'s second clause separately protects 'guidelines for law enforcement investigations or prosecutions if [their] disclosure could reasonably be expected to risk circumvention of the law.'" *Id.* (quoting 5 U.S.C. § 552(b)(7)(E)).

The "information withheld pursuant to Exemption [7(E)] includes computer screen transaction codes . . . [and] law enforcement techniques and procedures, which includes certain types of inspection, clearance, authorization procedures, and its results which, if disclosed, could be used to develop countermeasures to circumvent CBP operations and [the agency's] ability to enforce the laws of the United States." Second Pullo Decl. ¶ 27. More specifically, CBP relies on Exemption 7(E) to protect the following:

> (1) information relating to the TECS system and operating programs, including computer screen transaction codes, computer program transaction codes, and computer function codes (*e.g.*, 'PF codes' or 'navigation keys'); and (2) information contained in the system that reflects the results of specific law enforcement database queries (the 'RSLT' column).

Decl. of Dorothy Pullo [Dkt. #58-1] ("Third Pullo Decl."), Attach. to Mem. of Law in Supp. of Def.'s Renewed Mot. for Summ. J., Mar. 30, 2012, [Dkt. #58], ¶ 10; *see* Second Pullo Decl. ¶ 27.

CBP's declarant explains that, with respect "to computer screen transaction codes, computer transaction codes, and computer function codes," release of this information "facilitates access to and navigation through TECS and reveals mechanisms for access to and navigation through TECS." Third Pullo Decl. ¶ 11. The transaction codes "consist of the master record code and page record code," and thus, the declarant explains, "show precisely how information is retrieved from the database." *Id.* "Similarly, computer function codes reflect exact keys and keystrokes used for navigating TECS." *Id.* According to the declarant, if such computer code information were disclosed, an individual might obtain "[d]etailed knowledge about the system and its intricacies," which in turn "could lead individuals to alter their behavior to mislead law enforcement and avoid detection." *Id.* The declarant further states:

> [R]elease of this information could not only allow an individual knowledgeable in computer mainframes and systems to have unauthorized access (or hack) into the system, but also, once an unauthorized user has gained access to the system, knowledge of the withheld codes further facilitates the unauthorized user's ability to navigate through TECS. It would also arm unauthorized users with the ability to corrupt the integrity of the data contained therein through the alteration/manipulation of such data, which could leave to loss of the ability to timely recognize, detect, and apprehend certain individuals or otherwise detect and enforce against violations or attempts to violate the law. Similarly, if the system were to be hacked, knowledge of this information could permit the intruder to potentially manipulate the way certain records are created and maintained. Accordingly, public disclosure of such information could put at risk ongoing investigations and border security operations.

Id. ¶ 12. In short, in the agency's view, release of these computer codes "could reveal the precise procedures for retrieving records from a law enforcement database containing information related to [CBP's] law enforcement mission," and thus "expose the system to vulnerabilities and compromise the . . . data compiled for law enforcement purposes and other . . . missions." Second Pullo Decl. ¶ 26.

The RSLT column, the declarant explains, "contains codes and information reflecting the use, application, and results of certain types of inspection, clearance, and authorization procedures as utilized at the time of an individual's entry or exit from the United States." Third Pullo Decl. ¶ 13. Such "inherently law enforcement-related information, if disclosed, could be used to develop countermeasures to circumvent CBP operations and its ability to enforce the laws of the United States," the declarant states. *Id.* For example, release of this information "could reveal the names of law enforcement databases that were queried at the time of arrival and the results of those queries," and, it follows that disclosure of this information "reveal[s] CBP targeting and inspection techniques used in the processing of international travelers," such that "potential violators [could] design strategies to circumvent the examination procedures developed by CBP." *Id.* "[P]ut differently, individuals who knew the meaning of the codes contained in the 'RSLT' column would gain access to CBP law enforcement techniques and procedures that would permit them to alter their patterns of conduct, adopt new methods of operation, relocate, change associations, and effectuate other countermeasures, thus corrupting the integrity of ongoing investigations." *Id.*

"TECS is CBP's principal law enforcement and anti-terrorism database system, and it is one of the primary tools that CBP law enforcement officers . . . regularly use[] in order to effectively and efficiently enforce all particular laws, particularly [relating] to travelers and trade crossing the border into or out of the United States." *Id.* ¶ 14. It is "a fundamental law enforcement tool," for which "there is a great need to defend . . . against any threatened or real risk of threat or compromise, not only in order to ensure the continuance of CBP's mission, but in order to assist the other law enforcement agencies which TECS may support." *Id.*

Although the computer transaction and function codes are not themselves "techniques and procedures for law enforcement investigations or prosecutions" entitled to categorical protection under Exemption 7(E), the CBP's declarant adequately demonstrates that release of the codes, as well as the information in the RSLT column, "would disclose guidelines for law enforcement investigations or prosecutions[, and that] such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E). The CBP thus demonstrates that its decision to withhold the TECS-related information under Exemption 7(E) is proper. *See Skinner v. U.S. Dep't of Justice*, No. 09-cv-725, 2012 WL 4465788, at *3 (D.D.C. Sept. 28, 2012) (withholding "internal computer access codes associated with a hyper-sensitive law enforcement database containing homeland security information, *i.e.*, TECS"); *Miller v. U.S. Dep't of Justice*, No. 05-cv-1314, 2012 WL 2552538, at *13 (D.D.C. July 3, 2012) (withholding TECS numbers relating to procedures concerning use of law enforcement resources and databases and TECS case program and access codes on the ground that "disclosing [them] would expose a law enforcement technique, promote circumvention of the law by allowing criminals to conceal their activity, or allow fraudulent access to DEA's databases."); *McRae v. U.S. Dep't of Justice*, No. 09-cv-2052, 2012 WL 2428281, at *14 (D.D.C. June 27, 2012) (redacting "codes, case numbers, and other computer information pertaining to the TECS, NCIC, and databases maintained by the North Carolina authorities are techniques and procedures for law enforcement investigation"); *Bloomer* *v. U.S. Dep't of Homeland Sec.*, No. 5:11-cv-35, 2012 WL 1574468, at *8 (D. Vt. May 3, 2012) (redacting "various codes and case numbers," including the TECS Record ID, because disclosure of "internal instructions, codes, and guidance would reveal both a law enforcement technique and an internal investigative practice," which, in turn, "could endanger future investigations"); *cf. Soghoian v. U.S. Dep't of Justice*, No. 11-cv-1080, 2012 WL 3090309, at *10 (D.D.C. July 31, 2012) ("Knowing what information is collected, how it is collected, and more importantly, when it is *not* collected, is information that law enforcement might reasonably expect to lead would-be offenders to evade detection.").

IV. Segregability

FOIA requires that "[a]ny reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt." 5 U.S.C. § 552(b). "'It has long been the rule in this Circuit that non-exempt portions of a document must be disclosed unless they are inextricably intertwined with exempt portions.'" *Wilderness Soc'y v. U.S. Dep't of the Interior*, 344 F. Supp. 2d 1, 18 (D.D.C. 2004) (quoting *Mead Data Cent., Inc. v. U.S. Dep't of the Air Force*, 566 F.2d 242, 260 (D.C. Cir. 1977)). The CBP's declarant avers that she "conducted a line-by-line review of each record identified as responsive to [p]laintiff's FOIA request," Third Pullo Decl. ¶ 15, and has determined that "[a]ll information not exempted from disclosure . . . was correctly segregated and non-exempt portions were released," *id.* ¶ 16; Second Pullo Decl. ¶¶ 28-29. The CBP's declarations, coupled with a detailed Vaughn index, satisfy the Court that all reasonably segregable information has been disclosed to plaintiff. *See Abdelfattah v. U.S. Immigration & Customs Enforcement*, 851 F. Supp. 2d 141, 146 (D.D.C. 2012) (supplying an affidavit stating that documents were reviewed line-by-line, a sufficiently detailed Vaughn index, and declarations to explain why each document was properly withheld meets agency obligation regarding segregability).

CONCLUSION

The Court concludes that CBP properly has withheld information from the one-page document containing travel information about Stanley Ann Dunham, and defendants' renewed motion for summary judgment [Dkt. #58] therefore is GRANTED. Now that the Court has ruled on all motions and no matters are outstanding, and because each agency has demonstrated its compliance with the FOIA and entitlement to judgment as a matter of law, final judgment will be entered in favor of the defendants. An Order consistent with this Memorandum Opinion and with prior opinions and orders of this Court will be issued this same day.

RICHARD J. LEON
United States District Judge