

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

_____	)	
<b>SUSAN B. LONG, et al.,</b>	)	
	)	
<b>Plaintiffs,</b>	)	
	)	
<b>v.</b>	)	<b>Civil No. 14-00109 (APM)</b>
	)	
<b>IMMIGRATION AND CUSTOMS ENFORCEMENT, et al.,</b>	)	
	)	
<b>Defendants.</b>	)	
_____	)	

**MEMORANDUM OPINION AND ORDER**

This case arises from seven requests Plaintiffs Susan B. Long and David Burnham made under the Freedom of Information Act (“FOIA”) between October 13, 2010, and February 26, 2013, in which they sought information regarding the metadata and database schema for databases used by Defendant Immigration and Customs Enforcement (“ICE”) and Defendant Customs and Border Patrol (“CBP”), as well as information concerning “snapshots” of one database. Plaintiffs seek this information on behalf of the Transactional Records Access Clearinghouse (“TRAC”) at Syracuse University, which collects, organizes, and distributes data concerning federal government enforcement activities. Defendants produced several pages of responsive documents but withheld many others, leading to the present litigation. In a prior ruling in this matter, the court granted in part and denied in part the parties’ cross-motions for summary judgment.

Only a few issues in this litigation remain. First, the parties continue to dispute whether disclosure of metadata and database schema pertaining to Defendant ICE’s Enforcement Integration Database (“EID”) and Integrated Decision Support Database (“IIDS”) could reasonably be expected to risk circumvention of the law, such that those materials may be withheld

pursuant to FOIA Exemption 7(E). Second, the parties disagree as to whether Defendant conducted an adequate search to locate “snapshot” identification and preparation records, consistent with Plaintiffs’ Third FOIA Request, and then properly withheld certain responsive materials while segregating and releasing non-exempt materials. Both parties have moved for summary judgment.<sup>1</sup>

Despite an augmented record and supplemental briefing, summary judgment in full remains elusive. The court concludes that there remain genuine disputes of fact as to whether (1) disclosure of the EID and IIDS metadata and database schema could “*reasonably* be expected to risk circumvention of the law,” 5 U.S.C. § 552(b)(7)(E) (emphasis added); (2) the requested information concerning the timing and frequency of snapshot production was “compiled for law enforcement purposes” and, if so, whether its release could “*reasonably* be expected to risk circumvention of the law,” *id.* (emphasis added); and (3) whether Defendant performed a proper segregability analysis as to those responsive materials. The court does grant summary judgment to Defendant, however, as to the adequacy of its search in response to Plaintiffs’ Third FOIA Request, its withholding of employees’ names and contact information under Exemption 6, and its segregability analysis as to those withholdings. Accordingly, the court grants in part and denies in part Defendant’s Motion for Summary Judgment and denies in full Plaintiffs’ Cross-Motion for Summary Judgment.

---

<sup>1</sup> The court’s December 2015 Memorandum Opinion and Order granted summary judgment in favor of CBP on the issues pertaining to Plaintiffs’ Fifth and Seventh FOIA Requests, which were the only requests directed at CBP. *See Long v. Immigration & Customs Enf’t*, 149 F. Supp. 3d 39, 61 (D.D.C. 2015). The three FOIA Requests pertinent to this round of summary judgment only requested information from ICE. *See* Defs.’ Mot. for Summ. J., ECF No. 17, Attach. 3, ECF No. 17-3, at 1–3, 22–24, 48–52 (Exs. 1, 8 & 16). Accordingly, the court’s references to “Defendant” in this opinion pertain only to ICE.

## **I. BACKGROUND**

The court assumes the parties' familiarity with the underlying factual and procedural history of this case and recites only what is necessary to resolve the narrow issues that remain.

Three of Plaintiffs' seven FOIA requests are still at issue. Plaintiffs submitted two FOIA requests—one on October 13, 2010, the other on October 18, 2010—that sought documents disclosing the fields, variables, codes, and structures of the shared Enforcement Integration Database (“EID”) and Integrated Decision Support Database (“IIDS”), upon which ICE and CBP rely to manage cases pertaining to the detention of undocumented immigrants. *See Long v. Immigration & Customs Enf't*, 149 F. Supp. 3d 39, 43–44 (D.D.C. 2015). The EID contains information “related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by ICE, CBP, and U.S. Citizenship and Immigration Services.” *Id.* at 44 (alterations adopted) (internal quotation marks omitted). The IIDS contains a subset of that information, including “biographic information, information about encounters between agents/officers and subjects, and apprehension and detention information about all persons in EID,” which the agency uses to produce management and statistical reports. *Id.* at 45 (internal quotation marks omitted). Plaintiffs submitted a Third FOIA Request to Defendant on September 21, 2012, that sought, in relevant part, information relating to “snapshots” and extracts of the EID over a 12-month period. *Id.* “Snapshots” and extracts refer to subsets of select EID data maintained in other databases that allow Defendant to search all the information contained in the EID at a particular point in time. *Id.* Plaintiffs' Third FOIA Request seeks the following information surrounding these snapshots and extracts: (1) documents identifying any snapshots prepared in the past 12 months; (2) the

frequency with which snapshots are taken; (3) who prepares the snapshots; (4) to whom snapshots have been sent, and (5) how long it takes to prepare the snapshots. *See id.*

Plaintiffs received a limited amount of materials in response to these three FOIA requests. With respect to the first two requests, Defendant released 97 redacted pages of responsive documents, but withheld the remaining responsive materials premised on FOIA Exemption 7(E). *See id.* With respect to the Third FOIA Request, Defendant *created* a nine-page document (“the Nine-Page Document”) that summarizes the responsive materials and released a redacted version of that document, but not the original responsive materials. *See id.* at 46.

Plaintiffs filed suit, claiming, as relevant here, that Defendant has not complied with its FOIA obligations in responding to Plaintiffs’ request for EID and IIDS metadata and database schema or Plaintiffs’ Third FOIA Request. *See* Compl., ECF No. 1. Defendants moved for summary judgment on the ground that disclosure of EID and IIDS metadata and database schema would risk a Structured Query Language (“SQL”) injection attack, thereby justifying the agency’s withholding of that information under Exemption 7(E). *See* Defs.’ Mot. for Summ. J. & Mem. in Supp., ECF No. 17 [hereinafter Defs.’ Mot. for Summ. J., ECF No. 17], at 22–26.<sup>2</sup> Even assuming the materials sought could qualify for withholding under Exemption 7(E), Plaintiffs argued in opposition, it was unclear how Defendant could claim that disclosure of this information risks a SQL injection attack, given that that type of attack requires a direct connection to a database and the EID and IIDS are not publicly accessible. *See* Pls.’ Mem. in Supp. of Cross-Mot. for Summ. J., ECF No. 18, at 19. Separately, Plaintiffs noted, at no point had Defendant provided *any* information regarding its efforts to search for snapshot identification and preparation records in response to their Third FOIA Request. *See id.* at 31.

---

<sup>2</sup> Pin citations to this document reference the original pagination of Defendant’s Memorandum of Points and Authorities in Support, which begins on the third page of the document.

In a Memorandum Opinion and Order issued on December 14, 2015, the court agreed with Plaintiffs as to these two issues. Specifically, the court held that the metadata and database schema at issue satisfy the “compiled for law enforcement purposes” and “techniques, procedures, or guidelines” requirements of Exemption 7(E), but the court was unconvinced that Defendant had sufficiently shown how disclosure of these materials “could *reasonably* be expected to risk circumvention of law” in light of the incongruity between the type of harm claimed and the purported impossibility of it occurring. *See Long*, 149 F. Supp. 3d at 48–54 (emphasis added). Additionally, the court agreed that Defendant had not explained its efforts to conduct an adequate search for materials responsive to Plaintiffs’ Third FOIA Request. *Id.* at 60.

In the wake of the court’s decision, the parties submitted supplemental briefing and evidence in support of their respective positions. With respect to the EID and IIDS metadata and database schema, Defendant emphasized that its disclosure would risk circumvention of law even in the absence of a public interface because disclosing that information would make it easier for hackers to create convincing e-mails that lull unsuspecting, authorized users to click on nefarious links or attachments, also known as phishing or spear phishing attacks, and inadvertently allow hackers to access the system and/or steal users’ credentials. *See* Defs.’ Notice of Suppl. Evid., ECF No. 32 [hereinafter Defs.’ Notice], Ex. 3, ECF No. 32-3 [hereinafter Foster Decl.], ¶¶ 14–15; Defs.’ Suppl. Br. in Supp. of Defs.’ Mot. for Summ. J., ECF No. 35 [hereinafter Defs.’ Suppl. Summ. J. Br.], at 5–8. Separately, Defendant explains that the reasonableness and adequacy of its search in response to Plaintiffs’ Third FOIA Request is evidenced by the fact that the Request went through multiple levels of review, and experts in a sub-division curated the search and created a responsive document, with redactions justified under Exemptions 6, 7(C), and 7(E). Defs.’ Suppl. Summ. J. Br. at 16–17; Defs.’ Notice, Ex. 2, ECF No. 32-2 [hereinafter Wilson Decl.], ¶¶ 21, 25,

30, 35, 38, 49, 52. In response, Plaintiffs submitted a supplemental brief that contests the application of Exemption 7(E) to withhold the EID and IIDS metadata and database schema; the adequacy of the search in response to their Third FOIA Request; Defendant's reliance on Exemptions 6, 7(C), and 7(E) to withhold material responsive to the Third FOIA Request; and Defendant's segregability analysis. *See* Pls.' Suppl. Mem. in Opp'n to Defs.' Mot. for Summ. J. & in Supp. of Cross-Mot. for Summ. J., ECF No. 37 [hereinafter Pls.' Suppl. Summ. J. Br.]. In part, Plaintiffs argued that Defendant has identified no "reasonable" expectation that disclosure risks compromising EID security because Defendant previously provided to Plaintiffs earlier versions of the materials they now seek. *Id.* at 10–11. Because Defendants' supplemental reply brief did not respond to that argument, *cf.* Defs.' Opp'n to Pls.' Suppl. Cross-Mot. & Suppl. Reply Br. in Supp. of Defs.' Mot. for Summ. J., ECF No. 40 [hereinafter Defs.' Suppl. Reply], at 6–10, the court ordered supplemental briefing as to whether there remains a "reasonable" risk of a security breach given Plaintiffs' claim that Defendants previously disclosed the same type of information. Minute Order, Jan. 26, 2017.

The issues being ripe for resolution, the court now turns to the remaining issues in this litigation.

## **II. LEGAL STANDARD**

The court reviews *de novo* whether an agency has complied with its obligations under FOIA. 5 U.S.C. § 552(a)(4)(B).

On a motion for summary judgment, a court must enter judgment in favor of the moving party if that party "shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." FED. R. CIV. P. 56(a). A dispute is "genuine" only if a reasonable fact-finder could find for the nonmoving party, and a fact is "material" only if it is

capable of affecting the outcome of the litigation. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986).

FOIA requires a federal agency to conduct an “adequate search” in response to a FOIA Request. An agency performs an “adequate search” within the meaning of FOIA when it performs a search “reasonably calculated to uncover all relevant documents.” *Oglesby v. U.S. Dep’t of the Army*, 920 F.2d 57, 68 (D.C. Cir. 1990). The agency bears the burden of proving that it performed an adequate search and may rely on sworn affidavits or declarations to make that showing. *See SafeCard Servs., Inc. v. SEC*, 926 F.2d 1197, 1200 (D.C. Cir. 1991). The court may grant summary judgment to the agency based on those materials if they are reasonably specific and contradicted by neither other record evidence nor evidence of agency bad faith. *See Military Audit Project v. Casey*, 656 F.2d 724, 738 (D.C. Cir. 1981); *Beltranena v. Clinton*, 770 F. Supp. 2d 175, 181–82 (D.D.C. 2011). FOIA plaintiffs can rebut an agency’s declarations and affidavits by demonstrating that there remains a genuine issue as to whether the agency performed an adequate search for documents responsive to the plaintiff’s request. *See Hodge v. FBI*, 703 F.3d 575, 580 (D.C. Cir. 2013); *Span v. U.S. Dep’t of Justice*, 696 F. Supp. 2d 113, 119 (D.D.C. 2010) (internal quotation marks omitted).

The agency also bears the burden of proving that it withheld certain materials responsive to a plaintiff’s FOIA request pursuant to a statutory exemption. *Citizens for Responsibility & Ethics in Wash. v. U.S. Dep’t of Justice*, 746 F.3d 1082, 1088 (D.C. Cir. 2014). To make this showing, the agency, again, may rely on affidavits and declarations. If the agency’s materials “provide specific information sufficient to place the documents within the exemption category, if this information is not contradicted in the record, and if there is no evidence in the record of agency bad faith, then summary judgment is appropriate without in camera review of the documents.”

*Am. Civil Liberties Union v. U.S. Dep't of Def.*, 628 F.3d 612, 626 (D.C. Cir. 2011) (quoting *Larson v. U.S. Dep't of State*, 565 F.3d 857, 870 (D.C. Cir. 2009)).

Lastly, even when an exemption applies to shield one portion of a document responsive to the FOIA request, however, the agency is required to disclose “[a]ny reasonably segregable portion” of that document. *See* 5 U.S.C. § 552(b). “It is neither consistent with the FOIA nor a wise use of increasingly burdened judicial resources to rely on in camera review of documents as the principal tool for review of segregability disputes.” *Mead Data Cent., Inc. v. U.S. Dep't of the Air Force*, 566 F.2d 242, 262 (D.C. Cir. 1977) (footnote omitted). Instead, agencies enjoy a presumption of compliance with this obligation, absent contrary evidence submitted by the plaintiff. *See Sussman v. U.S. Marshals Serv.*, 494 F.3d 1106, 1117 (D.C. Cir. 2007).

### **III. DISCUSSION**

The court begins with whether Defendant may rely upon FOIA Exemption 7(E) to withhold the EID and IIDS metadata and database schema responsive to Plaintiffs’ first two FOIA requests before turning to the issues surrounding Defendant’s response to Plaintiffs’ Third FOIA Request.

#### **A. The EID and IIDS Metadata and Database Schema**

Defendant cites Exemption 7(E) to justify withholding the EID and IIDS metadata and database schema that Plaintiffs’ sought in their first two FOIA requests. That exemption protects 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.

552 U.S.C. § 552(b)(7)(E). Thus, to rely on this exemption when withholding information responsive to a FOIA request, the Government must demonstrate three things. First, the Government must show that the materials at issue are “records or information compiled for law enforcement purposes.” Then, the Government must show “that the withheld records or information ‘would disclose techniques and procedures for law enforcement investigations’” and “that their disclosure would reasonably ‘risk circumvention of the law.’” *Sack v. U.S. Dep’t of Defense*, 823 F.3d 687, 694 (D.C. Cir. 2016) (quoting 5 U.S.C. § 552(b)(7)(E)).

The court previously held that the EID and IIDS metadata and database schema are information compiled for law enforcement purposes that qualify at least as law enforcement guidelines, if not also law enforcement methods and techniques, , but it was not clear whether disclosure of the materials at issue could *reasonably* be expected to risk circumvention of the law. *Long*, 149 F. Supp. 3d at 49–50, 53; Minute Order, Jan. 26, 2017. Each party now moves for summary judgment as to that issue.

Whether disclosure “could *reasonably* be expected to risk circumvention of the law” is a fairly low hurdle in this Circuit, but it is not a toothless standard. The Government need only “demonstrate logically how the release of the requested information might create a risk of circumvention of the law.” *Blackwell v. FBI*, 646 F.3d 37, 42 (D.C. Cir. 2011) (quoting *Mayer Brown LLP v. IRS*, 562 F.3d 1190, 1194 (D.C. Cir. 2009)).

The exemption looks not just for circumvention of the law, but for a risk of circumvention; not just for an actual or certain risk of circumvention, but for an expected risk; not just for an undeniably or universally expected risk, but for a reasonably expected risk; and not just for certitude of a reasonably expected risk, but for the chance of a reasonably expected risk.

*Id.* (quoting *Mayer Brown*, 562 F.3d at 1193); accord *Public Employees for Env’tl Responsibility v. U.S. Section, Int’l Boundary & Water Comm’n, U.S.–Mexico*, 740 F.3d 195, 205 (D.C. Cir.

2014) (explaining that the Government “must demonstrate only that release of a document *might* increase the risk that a law will be violated or that past violators will escape legal consequences” to successfully rely on Exemption 7(E) (emphasis added)). Nonetheless, the Government cannot simply cite Exemption 7(E) and expect the court to rubber stamp its withholdings. *Cf., e.g., Citizens for Responsibility & Ethics in Wash.*, 746 F.3d at 1102 (denying summary judgment where agency had simply parroted the language of the exemption). At a minimum, the Government must show that its stated expectation of risk is reasonable. Though the risk need not be “undeniably or universally expected,” it must be “reasonably expected”; though “certitude of a reasonably expected risk” need not be shown, there must be evidence of “the chance of a reasonably expected risk.” *Mayer Brown*, 562 F.3d at 1193. Thus, reasonableness is the keystone of Exemption 7(E).

Defendant’s supplemental filings introduce a new set of potential risks that Defendant claims disclosure would create. Rather than focus on the risk of a SQL injection attack, as Defendant did during the initial round of summary judgment briefing, Defendant’s supplemental briefs represent that disclosure would risk e-mail-based attacks—such as phishing, spear phishing, and advanced persistent threat intrusions (“APT attacks”)—that could harm its systems, given that the more information a hacker has about the targeted system, the easier it is to lull unsuspecting, authorized users to click on nefarious links or attachments in e-mails, allowing access to the system and theft of authorized users’ credentials. *See* Defs.’ Suppl. Summ. J. Br. at 5–8; Defs.’ Suppl. Reply at 9; Foster Decl. ¶¶ 14–15.<sup>3</sup> Providing the information Plaintiffs requested would undermine its “defense in depth” security strategy, in which it buries information about the system to prevent attackers from having the information that allows them to mount successful phishing

---

<sup>3</sup> Defendant makes clear in its Supplemental Reply Brief that it has not abandoned its position that a SQL attack is possible and made more likely through disclosure of the metadata and database schema. *See* Defs.’ Suppl. Reply at 4. Instead, it argues that disclosure of these materials risks not only a SQL attack, but also these types of e-mail-based attacks. *See id.*

and spear-phishing attacks. Defs.’ Suppl. Summ. J. Br. at 10–11; Foster Decl. ¶¶ 9–10. Additionally, release of this information would place other agencies’ systems at risk, because once one system suffers a successful hack, any other connected system also can be breached. *See* Defs.’ Suppl. Summ. J. Br. at 11. Furthermore, any prior disclosure of this information, Defendant claims, was entirely “inadvertent.” Defs.’ Second Suppl. Br., ECF No. 44 [hereinafter Defs.’ Second Suppl. Br.], at 1; *see* Defs.’ Second Suppl. Br., Ex. 1, ECF No. 44-1 [hereinafter Wilson Suppl. Decl.], ¶¶ 7–8, 12.<sup>4</sup>

Plaintiffs’ supplemental filings aver that Defendant’s assessment of the risk posed by disclosure is illogical in light of the lack of an external access point to the system and Defendant’s past practice of releasing copious amounts of materially indistinguishable information. Plaintiffs submit that hackers do not need the metadata and database schema to launch an e-mail-based attack, but even if that information was disclosed, any risk of circumvention of law still depends on Defendant’s system having some external access point, such as a web-based interface or internet connection, that would allow the hacker to remotely access or control the system—which Defendant’s system does not have. *See* Pls.’ Suppl. Summ. J. Br. at 3–5, 8–9. Additionally, Plaintiffs assert, any stated expectation of risk of circumvention of law is disingenuous because Defendant has previously provided Plaintiffs with the very information it is now withholding. *See id.* at 10–11. Specifically, Plaintiff Long submits that, since 2008, “[o]n more than a *hundred* occasions,” Defendant released “the specific categories of information that [D]efendant[] now claim[s] create a serious security breach.” Pls.’ Second Suppl. Mem., ECF No. 45 [hereinafter Pls.’ Second Suppl. Br.], Ex. 1, ECF No. 45-1 [hereinafter Fourth Long Decl.], ¶¶ 4, 5 (emphasis

---

<sup>4</sup> Defendant frames the issue of prior disclosures in terms of waiver, *see* Defs.’ Second Suppl. Br. at 2, but that is incorrect; the issue is whether Defendant’s prior disclosures affect the reasonableness of the expected risk of harm from subsequent disclosures of materially indistinguishable information.

added). The information previously disclosed includes “technical documentation concerning the EID and IIDS databases, including data field and table names, database schema, code translation tables and other technical information including actual code values.” *Id.* ¶ 5. Indeed, Defendant *has continued* to supply this information in response to other outstanding FOIA requests Plaintiff has submitted. In or about February 2017, Plaintiffs “received thirteen new releases with the equivalent of thousands of pages containing actual database field names, the actual contents of database auxiliary lookup tables and countless actual code values—the very information that the defendant claims poses a serious risk of a security breach.” *Id.* ¶ 12. Accordingly, Plaintiffs conclude, any expected risk of circumvention of law is not “reasonable,” given the agency’s consistent and fulsome release of this information for roughly the last ten years, including throughout the length of this litigation.

The court concludes that summary judgment is inappropriate because Defendant’s affidavits do not state in any level of detail how a hacker could access a system with no external access point, and Plaintiffs have introduced specific facts that contradict Defendant’s statements that all prior releases of this information were inadvertent. *See Am. Civil Liberties Union*, 628 F.3d at 626. These uncertainties on the record create a triable issue of fact as to the reasonableness of Defendant’s expectation of risk of circumvention of the law. *See Sears, Roebuck & Co. v. Gen. Servs. Admin.*, 553 F.2d 1378, 1382 (D.C. Cir. 1977) (explaining that summary judgment is inappropriate when the affidavits before the court reflecting conflicting views on the adverse consequences flowing from disclosure of the withheld materials).

First, it remains unclear to the court what role, if any, an external access point plays in determining the risk of circumvention of law flowing from disclosure of the EID and IIDS metadata and database schema. The means of access to the EID has been a point of contention

throughout the litigation, *see Long*, 149 F. Supp. 3d at 53, 61, and even after substantial briefing, it remains ambiguous to the court whether the EID can be externally or remotely accessed and, if not, how a hacker could gain access to it through a SQL or e-mail-based attack. These questions are material because Defendant's argument centers on the fact that a circumvention of law only occurs when the hacker *accesses* the database. *See* Defs.' Suppl. Summ. J. Br. at 8. If there is no means of accessing the database, then Defendant's expectation that disclosure of the EID and IIDS metadata and database schema will risk circumvention of the law is not reasonable. Although Defendant continuously repeats that access to the EID is possible even in the absence of an external access point, *see id.* at 9, 12, Defendant has offered no explanation for how that would occur. At most, Defendant indicates that disclosure of the withheld materials would allow a hacker to study the database. But, what then? The court could infer from Defendant's submissions that the EID is connected to another government database that has an external access point and that interconnection makes the EID vulnerable, but that is impermissible speculation on the court's part. Defendant has not identified any database that is connected to the EID, has an external access point, and is vulnerable to attack. *Cf.* Foster Decl. ¶¶ 19–21 (describing other systems as being “interconnect[ed]” to the EID, allowing for “interoperability among the various Agency systems,” but not describing any other system as having an external access point); Defs.' Suppl. Summ. J. Br. at 12. This Circuit demands that the Government “demonstrate *logically* how the release of the requested information might create a risk of circumvention of the law.” *Blackwell*, 646 F.3d at 42 (emphasis added). On the present record, there is a logical gap in Defendant's reasoning.

Second, there remains a genuine dispute of fact as to whether Defendant's reasons for withholding the present information are manufactured or legitimate in light of Defendant's past practice of disclosing EID and IIDS metadata and database schema. As a general matter, a federal

agency's disclosure of certain information at one point in time does not prevent the agency from concluding at a later date that disclosure of the same information gives rise to a "reasonably" expected risk of unlawful activity. Intuitively, it is clear that circumstances and an agency's assessment of threats change over time. Moreover, clerical errors—such as inadvertently disclosing a few unredacted pages amidst thousands of pages of properly processed materials—do not reflect on either the agency's assessment of the sensitivity of the inadvertently disclosed documents or the legitimacy of the previous decision to withhold those documents, and the court will not assume such errors are made in bad faith. *Cf. Kay v. Fed. Commc'ns Comm'n*, 867 F. Supp. 11, 23–24 (D.D.C. 1994) (concluding that, for purposes of FOIA Exemption 7(A), the FCC's inadvertent release of six unredacted letters amidst a 1,474-page disclosure did not make the FCC's prior withholding of those six letters arbitrary and capricious, or otherwise in bad faith, in the absence of any evidence to the contrary). A situation in which an agency makes a single, intentional disclosure—or a single, inadvertent disclosure—followed by a subsequent decision to withhold the material in the future is fundamentally different in kind, though, from one in which the agency, for years, discloses a certain type of information in response to FOIA requests and then subsequently claims that information should have been withheld and all prior disclosures were "inadvertent." That latter circumstance is undoubtedly further complicated when the agency continues to make those voluminous, "inadvertent disclosures" throughout the very litigation in which it seeks a judgment in its favor that the information it is actively disclosing may be properly withheld.

On the present record, the court cannot discern the character of Defendant's past disclosures of metadata and database schema. Defendant's affiant, Jeff Wilson—the Unit Chief of the Information Technology Management Unit, which operates within the Enforcement and

Removal Operations Law Enforcement Systems and Analysis (“LESA”) division at ICE—states that Defendant “first became aware of the inadvertent releases [of the EID and IIDS metadata and database schema] through an additional FOIA request submitted by Plaintiffs at or around [June 2013],” leading to review of those “inadvertently released” documents and remedial training of LESA staff. *See* Wilson Suppl. Decl. ¶¶ 9–10. Plaintiff Long’s affidavit, however, contradicts Defendant’s version of events:

ICE’s past releases of the specific categories of information that defendants now claim create a serious security breach cannot be described as accidental, unintentional, or inadvertent. They were not simply the result of an inadequately trained office clerk. On more than a hundred occasions, these releases occurred only after TRAC took an administrative appeal to the head of the agency (sometimes with the support of legal arguments presented by an attorney) and received a decision by ICE’s Office of the Principal Legal Advisor. A number of releases of materials the government now claims pose a serious security risk only occurred after review at the Department of Homeland Security headquarters when we sought its review of the matter. . . .

[D]efendants on numerous occasions disclosed technical documentation concerning the EID and IIDS databases, including data field and table names, database schema, code translation tables and other technical information including actual code values, without any suggestion that these disclosures risked cyber-attacks. Such releases began as far back as 2008 and have continued. . . . These releases . . . were prepared by staff of the Enforcement and Removal Operations (“TRO”) Law Enforcement and Systems Analysis (“LESA”) office in which [D]efendants’ declarant, Mr. Wilson, is employed. Further, releases that only took place after appeal to the head of the agency occurred throughout this entire period *and have continued up until present*.

. . . .

Defendants’ disclosures of identical types of records have been extensive—indeed massive. They have also been ongoing and have continued to the present. For example, *in the last thirty days*, in response to TRAC’s FOIA requests to ICE for current information we have received thirteen new releases with the equivalent of thousands of pages containing actual database field names, the actual contents of database auxiliary lookup tables, and countless

actual code values—the very information that the defendant claims poses a serious risk of a security breach. Given the volume of our requests, this volume of releases is not unusual.

Fourth Long. Decl. ¶¶ 4–5, 12 (emphases added). Wilson’s and Long’s sworn statements are irreconcilable. Plaintiffs’ representations that Defendant not only has disclosed large amounts of functionally indistinguishable information to that being currently withheld, but also has done so for nearly ten years—with the most recent disclosure occurring in February 2017—directly contravene Defendant’s statement that the disclosures of the EID and IIDS metadata and database schema was entirely “inadvertent” and the agency has acted to prevent such disclosures since June 2013. Defendant has not attempted to distinguish the materials previously disclosed in any way from the presently withheld materials. At most, Mr. Wilson states that the materials being withheld are “new” because the requested metadata and database schema are part of a “live system that adds and removes information over time,” such that the information inadvertently released in the past is different than the information sought today. *See* Wilson Suppl. Decl. ¶¶ 12–13. But that statement is hardly satisfactory, as Mr. Wilson offers no factual detail showing how and to what extent the metadata and database schema at issue actually differs from that released in the past or how the character of that new information reasonably risks a violation of the law. Additionally, Defendant offers no response to Plaintiffs’ assertion that it has disclosed large quantities of metadata and database schema throughout this litigation, as recently as seven months ago.

These disputed facts are material because if Defendant has been knowingly and intentionally disclosing EID and IIDS metadata and database schema for years, including during the present litigation, then that would call into question the reasonableness of Defendant’s expectation that disclosure of the presently withheld information could contribute to or increase the risk of phishing, spear phishing, APT attacks, or SQL attacks. Absent some distinguishing

feature between the previously disclosed information and the information being shielded here, or some other explanation for the prior release of indistinguishable information, it arguably would be patently *unreasonable* to claim an expected risk of attack from disclosing the presently withheld materials. Indeed, if there is no difference between the materials being continuously disclosed—for years prior to and in the background of this very litigation—and the EID and IIDS metadata and database schema at issue here, then Defendant itself would be contributing to the expected risk of unlawful activity through such disclosures.

In sum, the court cannot hold, based on the genuine disputes of material fact the record presents, that Defendant’s expectation of risk of circumvention of law flowing from disclosure of the EID and IIDS metadata and database schema is reasonable. Accordingly, the court denies both Defendant’s Motion and Plaintiffs’ Cross-Motion for Summary Judgment as to the applicability of Exemption 7(E) to withhold the EID and IIDS metadata and database schema.

**B. Plaintiffs’ Third FOIA Request**

By letter dated September 21, 2012, Plaintiffs submitted the following FOIA request to Defendant:

Under the provisions of the Freedom of Information Act we request a copy of records identifying any extracts and “snapshots” prepared from the Enforcement Integrated Database (EID) over the last 12 months, along with records relating to the frequency with which such extracts and snapshots have been prepared, who was responsible for preparing any snapshot or extract, the recipient(s) of that extracts/snapshots [sic], as well as the EID system time required in their preparation during this period.

Defs.’ Mot. for Summ. J., ECF No. 17, Attach. 3, ECF No. 17-3, at 42–43 (Ex. 14). Defendant interpreted this request as seeking five categories of materials: “(a) documents identifying extracts and ‘snapshots’ prepared for the previous 12 months; (b) records related to the frequency with which extracts/snapshots are prepared; (c) the individuals responsible for preparing

extracts/snapshots; (d) documents identifying the recipient(s) of the extract/snapshots; and (e) the amount of time it takes the EID system to prepare reports.” Defs.’ Suppl. Summ. J. Br. at 15.

In response to this Request, Defendant created the Nine-Page Document and released a redacted version of it to Plaintiffs, but did not disclose, in whole or in part, any original, responsive materials. The Nine-Page Document is “not a document that is kept or maintained by [Defendant] in its normal course of business,” but instead, a document created specifically in response to Plaintiffs’ Request. Wilson Decl. ¶¶ 5–6; *accord* Defs.’ Notice, Ex. 1, ECF No. 32-1 [hereinafter Pineiro Decl.], ¶ 17; *see also* Defs.’ Mot. for Summ. J., ECF No. 17, Attach. 3, ECF No. 17-3, at 55–66 [hereinafter Nine-Pg. Doc.].

In the last Memorandum Opinion, the court denied Defendant’s Motion for Summary Judgment as to the adequacy of its search for records responsive to Plaintiffs’ Third FOIA Request because Defendant failed to explain what search, if any, it undertook. *Long*, 149 F. Supp. 3d at 59–60. Following that ruling, Defendant submitted supplemental evidence and briefing regarding the scope of the search it performed and the FOIA exemptions upon which it relies to justify withholding certain materials responsive to that Request. The parties now move for summary judgment as to the adequacy of the search, the appropriateness of Defendant’s redactions and withholdings from the Nine-Page Document, and whether Defendant performed a proper segregability analysis when creating the Nine-Page Document.<sup>5</sup>

The court addresses the adequacy of Defendant’s search before turning to the appropriateness of its reliance on Exemptions 6, 7(C), and 7(E) to withhold responsive materials and the sufficiency of its segregability analysis.

---

<sup>5</sup> Plaintiff has not argued expressly that Defendant violated FOIA by responding to the Third FOIA Request with the Nine-Page Document rather than releasing all the responsive documents, with redactions. Thus, that issue is not before the court.

*I. Adequacy of the Search in Response to Plaintiffs' Third FOIA Request*

Defendant has supplemented the record with two affidavits that outline the steps it took upon receiving Plaintiffs' Third FOIA Request and how it created the Nine-Page Document. *See* Defs.' Suppl. Summ. J. Br. at 16–18; Wilson Decl.; Pineiro Decl.

Defendant's first affiant, Fernando Pineiro, the Deputy FOIA Officer of ICE's FOIA Office, explains the process Defendant undertook in response to Plaintiffs' Third FOIA Request, and Defendant's second affiant, Jeff Wilson, the Unit Chief of the Information Technology Management Unit in the LESA Unit, describes why a separate search was unnecessary. Mr. Pineiro describes Defendant's efforts to respond to Plaintiffs' Third FOIA Request as follows. First, the ICE FOIA Office assessed each of the five sub-categories of information sought in Plaintiffs' Request and determined that the ICE Office of Enforcement and Removal Operations ("ERO") would be best able to identify responsive records. Pineiro Decl. ¶ 9. Accordingly, the ICE FOIA Office tasked ERO with conducting a search and sending back any records responsive to the search. *Id.* ERO's Information Disclosure Unit reviewed Plaintiffs' Request, determined subject matter experts in the LESA Unit at ICE Headquarters should conduct the search, and sent the Request to LESA. *Id.* ¶ 12. LESA experts, in turn, sent the request to the Office of the Chief Information Officer ("OCIO"), believing OCIO was in a better position to respond. *Id.* With authorization from the ICE FOIA Office to conduct a comprehensive search, OCIO reviewed Plaintiffs' Request and determined that subject matter experts in the Systems Development Division should conduct the search. *Id.* ¶¶ 13, 16. OCIO's search, performed by the experts in the Systems Development Division, resulted in the partially redacted Nine-Page Document Plaintiffs subsequently received on January 25, 2013. *Id.* ¶ 17. Mr. Wilson notes that the Division did not conduct a separate search of the System Lifecycle Management ("SLM") repository in response

to Plaintiffs' Third FOIA Request on the belief that such a search would needlessly duplicate agency efforts and fail to produce the information Plaintiffs are seeking. Specifically, he explains that the SLM repository was thoroughly searched in connection with Plaintiffs' first two FOIA Requests and all responsive materials were catalogued in the Supplemental *Vaughn* Index and Amended Detailed Description Table, making another search of the same source redundant. *Id.* ¶¶ 11–12. Further, the SLM repository purportedly does not contain any information regarding (1) who monitors the automated processes of preparing and receiving the extracts and snapshots, or (2) the amount of time it takes to prepare a snapshot or extract. *See id.* ¶¶ 7–8, 13. Instead, Defendant asked individuals with institutional knowledge of ICE to provide the names of those who monitor the process of preparing and receiving the extracts and snapshots. *Id.* at ¶ 7. Additionally, because Defendant “only maintains a record of fixed start times for extra preparations in the technical documentation,” any timing information contained in the Nine-Page Document released to Plaintiffs was provided by those with institutional knowledge or “otherwise extrapolated from system audit logs.” *Id.* ¶ 8.

In light of these additional affidavits, the court is satisfied that Defendant met its burden of proving it performed an adequate search in response to Plaintiffs' Third FOIA Request. The court previously ruled that Defendant performed an adequate search in response to Plaintiffs' first two FOIA Requests by searching the SLM repository, *Long*, 146 F. Supp. 3d at 60–61, and Plaintiffs offer no argument during this round of summary judgment briefing to rebut Defendant's affiant's statement that all records responsive to Plaintiffs' Third FOIA Request would have been uncovered when performing that search. Instead, Plaintiffs' arguments focus on whether Defendant was required to provide a new *Vaughn* Index that identifies the responsive records on which it relied when creating the Nine-Page Document or explain in greater detail the basis for its withholdings.

*See* Pls.’ Suppl. Summ. J. Br. at 13–14. These arguments, however, pertain to the appropriateness of Defendant’s withholdings from the Nine-Page Document, not the adequacy of its search for materials to create the Nine-Page Document. In the face of the court’s prior decision and the absence of any counter argument, the court concludes Defendant performed an adequate search in response to Plaintiffs’ Third FOIA Request. Accordingly, the court grants Defendant’s Motion for Summary Judgment as to the adequacy of its search in response to Plaintiffs’ Third FOIA Request.

2. *Defendant’s Reliance on Exemptions 6, 7(C), and 7(E) to Withhold Materials Responsive to Plaintiffs’ Third FOIA Request*

The heart of Plaintiffs’ challenge to Defendant’s response to Plaintiffs’ Third FOIA Request concerns whether Defendant properly invoked FOIA Exemptions 6, 7(C), and 7(E) to withhold material from the Nine-Page Document that was responsive to that Request. Three of the categories of information Plaintiffs seek in their Third FOIA Request concern the timing and frequency of snapshots, while the other two categories pertain to identifying information of individuals who prepare or receive snapshots. *See* Defs.’ Suppl. Summ. J. Br. at 15. Defendant relies on FOIA Exemption 7(E) to withhold information concerning the timing and frequency of snapshots, as well as the names of the law enforcement systems that interact with a particular EID module. *See Vaughn* Index at 8 (No. 14); Defs.’ Suppl. Summ. J. Br. at 18–20, 24–26. Additionally, Defendant relies on Exemptions 6 and 7(C) to withhold the names, phones numbers, and e-mail addresses of employees who manage the systems with which the EID module interacts. *Vaughn* Index at 8 (No. 14); Defs.’ Suppl. Summ. J. Br. at 21–24.

To determine whether the Nine-Page Document Defendant created in response to Plaintiffs’ Third FOIA Request may be withheld under any provision of FOIA Exemption 7, the court must first determine whether the document is a “record[] or information compiled for law

enforcement purposes.” 5 U.S.C. §552(b)(7).<sup>6</sup> To be compiled for a law enforcement purpose, there must be (1) a rational “nexus” between the record and the agency’s law enforcement duties and (2) a connection between the subject of the record and a “possible security risk or violation of federal law.” *Campbell v. U.S. Dep’t of Justice*, 164 F.3d 20, 32 (D.C. Cir. 1998). The fact that Defendant created the Nine-Page Document in response to Plaintiffs’ FOIA Request does not render it ineligible for Exemption 7’s protection. Rather, “information initially contained in a record made for law enforcement purposes continues to meet the threshold requirements of Exemption 7 where that recorded information is reproduced or summarized in a new document prepared for a non-law-enforcement purpose.” *FBI v. Abramson*, 456 U.S. 615, 631–32 (1982). Thus, whether the Nine-Page Document may be withheld in whole or in part under Exemption 7(C) or 7(E) depends on whether the documents excerpted or summarized therein were compiled for law enforcement purposes.

Although the record contains the Nine-Page Document, the amended *Vaughn* Index, Mr. Pineiro’s recounting of the search that led to the creation of the Nine-Page Document, and Mr. Wilson’s description of what categories of materials were responsive to Plaintiffs’ Third FOIA Request, the court still cannot discern what materials contributed to the Nine-Page Document and, correlatively, whether those materials were compiled for law enforcement purposes.

To begin, neither the Nine-Page Document itself nor the *Vaughn* Index description of it sheds any light on the materials on which Defendant relied in creating the Nine-Page Document. The Nine-Page Document contains no index or other citations to the materials on which it relies. Instead, it contains a two-page overview of the sub-systems and “data marts” that collect categories

---

<sup>6</sup> Contrary to Defendant’s assertion, the court did not previously hold that all materials responsive to Plaintiffs’ Third FOIA Request are compiled for law enforcement purposes. *Contra* Defs.’ Suppl. Reply Br. at 18. The court only determined that records responsive to Plaintiffs’ other FOIA Requests, pertaining to the EID and IIDS metadata and database schema, were compiled for law enforcement purposes. *See Long*, 149 F. Supp. 3d at 48–49.

of data through the EID, as well as descriptions of those categories of data, followed by seven pages of partially redacted information regarding the timing and frequency of data updates, as well as the names and contact information of the creators and recipients of that data. *See* Nine-Pg. Doc. Defendant's *Vaughn* Index proves similarly unhelpful. The Index, both originally and as amended, consistently refers to the Nine-Page Document as "12-24067 Redacted Combined" and describes it as: "EARM Interfaces Summary for FOIA Request. This document provides a description of the Enforcement Integrated Database (EID) and explains how one of its modules, the Enforcement Alien Removals Module (EARM), connects with other law enforcement databases." Notice of Filing *Vaughn* Index, ECF No. 10, *Vaughn* Index, ECF No. 10-1 [hereinafter *Vaughn* Index], at 8 (No. 14); Notice of Filing Suppl. *Vaughn* Index, ECF No. 24, Am. *Vaughn* Index, ECF 24-2, at 10 (No. 14); Defs.' Opp'n to Pls.' Cross-Mot. for Summ. J., ECF No. 25, Attach. 5, ECF No. 25-5 [hereinafter Am. *Vaughn* Index], at 10 (No. 14). Consequently, neither the original Nine-Page Document nor the *Vaughn* Index indicates the materials that comprise the Nine-Page Document.

Defendants' affiants do not offer any further details. Although Mr. Pineiro explains the steps undertaken to search for records responsive to Plaintiffs' Third FOIA Request, he does not identify or describe the responsive materials on which OCIO relied when creating the Nine-Page Document. *See* Pineiro Decl. ¶¶ 6–17. Separately, Mr. Wilson identifies five types of records that contain information responsive to all the sub-categories of documents sought in Plaintiffs' Third FOIA Request. *See* Wilson Decl. ¶¶ 15, 22, 28, 36, 44.<sup>7</sup> All the categories Mr. Wilson identifies are generically described in Defendant's Amended Detailed Description Table, but neither Mr. Wilson nor the Table identifies which categories of materials contributed to or otherwise informed the creation of the Nine-Page Document. *See id.*; Notice of Filing Suppl. *Vaughn* Index,

---

<sup>7</sup> Mr. Wilson also lists more than 50 other categories of documents in which information relating to the frequency and timing of snapshots might be found. *See* Wilson Decl. ¶¶ 16, 23, 45.

ECF No. 13, Detailed Description Tbl., ECF No. 13-1; Defs.' Mot. for Summ. J., ECF No. 17, Attach. 4, ECF No. 17-4; Notice of Filing Suppl. *Vaughn* Index, ECF No. 24, Am. Detailed Description Tbl., ECF No. 24-1; Defs.' Opp'n to Pls.' Cross-Mot. for Summ. J., ECF No. 25, Attach. 4, ECF No. 25-4.

In the absence of any evidence indicating what materials or documents were relied upon to create the Nine-Page Document and whether those materials or documents were compiled for law enforcement purposes, the court cannot discern if any portion of the Nine-Page Document is eligible to be withheld pursuant to FOIA Exemption 7. Accordingly, the court denies both parties' motions for summary judgment concerning the applicability of Exemptions 7(C) and 7(E) to withhold portions of the Nine-Page Document relating to the timing and frequency of snapshots or the names and contact information of those who create or receive snapshots.<sup>8</sup>

The court is able, however, to resolve whether Defendant properly invoked Exemption 6 to withhold the identifying information of individuals that prepare or receive snapshots. FOIA Exemption 6 allows the Government to withhold materials responsive to a FOIA request if those materials include "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6). To determine if Exemption 6 applies, the court follows a two-step inquiry that tracks the statutory

---

<sup>8</sup> The court notes that, even were the court to assume the Nine-Page Document was created from materials compiled for law enforcement purposes, the court would be unable to determine whether Defendant properly invoked Exemption 7(E) to withhold those portions of the Nine-Page Document relating to the timing and frequency of snapshots. Defendant relies on the same rationale to withhold that information as it does to withhold the materials responsive to Plaintiffs' first two FOIA Requests. Generally, Defendant contends that releasing information concerning the timing and frequency of snapshots would put in hackers' hands too much information about Defendant's systems and render those systems susceptible to attack. *See* Defs.' Suppl. Summ. J. Br. at 19–20, 25–26; Defs.' Suppl. Reply at 19. Plaintiffs, for their part, offer the same counter-argument: Defendant cannot claim a reasonable risk of circumvention of law exists when Defendant previously disclosed the information at issue and has not identified how an attack could occur in the absence of an external access point. *See* Pls.' Suppl. Summ. J. Br. at 17–22. On the present record and faced with the same arguments, the court would be in no better position to assess whether there is a reasonable risk of circumvention of law from the disclosure of these materials than from the disclosure of the EID and IIDS metadata and database schema.

language. The court first “determine[s] whether the records are personnel, medical, or ‘similar’ files covered by Exemption 6,” and, if so, then “determine[s] whether their disclosure ‘would constitute a clearly unwarranted invasion of personal privacy.’” *Am. Immigration Lawyers Ass’n v. Executive Office for Immigration Rev.*, 830 F.3d 667, 673 (D.C. Cir. 2016) (alterations adopted) (quoting *Multi Ag Media LLC v. U.S. Dep’t of Agric.*, 515 F.3d 1224, 1228 (D.C. Cir. 2008)). Under the latter step, the court must engage in a balancing test to determine whether the public interest in disclosure is outweighed by a significant private interest in non-disclosure. *Id.*

The names and contact information of federal employees are the type of information that is eligible for withholding under Exemption 6. Although Exemption 6 “does not categorically exempt individuals’ identities” from disclosure, it has been construed broadly enough to allow an agency “to exempt not just files, but also bits of personal information, such as names and addresses,” provided the disclosure “would create a palpable threat to privacy.” *Judicial Watch, Inc. v. FDA*, 449 F.3d 141, 152–53 (D.C. Cir. 2006) (alteration adopted) (internal quotation marks omitted); accord *Calderon v. U.S. Dep’t of Agric.*, 236 F. Supp. 3d 96 (D.D.C. 2017) (explaining that the threshold for applying Exemption 6 is met if the information “applies to a particular individual” (quoting *U.S. Dep’t of State v. Wash. Post Co.*, 456 U.S. 595, 602 (1982))). The fact that an individual is a federal employee does not change that analysis. See, e.g., *Schoenman v. FBI*, 575 F. Supp. 2d 136, 160 (D.D.C. 2008); *Elec. Privacy Info. Ctr. v. U.S. Dep’t of Homeland Sec.*, 384 F. Supp. 2d 100, 116 (D.D.C. 2005). Consequently, federal employees’ personal identifying information is of the type that Exemption 6 potentially allows to be withheld.

The court holds that Defendant properly invoked Exemption 6 to withhold the names and contact information of those individuals who prepare and receive snapshots of the EID because the public interest in disclosure does not outweigh the individuals’ privacy interest in

nondisclosure. Defendant's affiant explains that publicly identifying by name, telephone number, of e-mail address those individuals responsible for the particular, sensitive task of monitoring snapshots of the EID would subject those individuals to targeted, unauthorized, and potentially malicious inquiries about their work; even harassment. Wilson Decl. ¶ 32, 41–42. The court agrees that federal employees have a legitimate privacy interest in avoiding targeted harassment based on their role in monitoring and receiving EID snapshots and, further, that withholding a telephone number or e-mail address, alone, is not sufficient to protect that interest; alternate means of contacting and harassing these employees would be readily discoverable on the Internet if this court ordered their names disclosed. *Cf. Judicial Watch, Inc.*, 449 F.3d at 153 (explaining that individuals have a privacy interest in the nondisclosure of their names and addresses in order to avoid physical danger). Plaintiffs advance no opposing public interest in knowing these employees' names and addresses. Indeed, they assert only that Defendant previously disclosed federal employees' names and should not be able to withhold that same information now. *See* Pls.' Suppl. Summ. J. Br. at 19; *see* Pls.' Suppl. Summ. J. Br., Attach. 1, ECF No. 37-1, ¶ 9. In the face of a legitimate privacy interest in nondisclosure and the absence of any countervailing public interest in disclosure, the court concludes Defendant properly withheld the federal employees' names and contact information. *See Schoenman*, 575 F. Supp. 2d at 161 (holding, in the context of Exemption 6, that where the defendant had identified a slightly-greater-than-de minimis privacy interest and the court found no public interest existed "something, even a modest privacy interest[,] outweighs nothing every time" (quoting *Nat'l Ass'n of Retired Fed. Emps. v. Horner*, 879 F.2d 873, 879 (D.C. Cir. 1989))).

Consequently, the court grants Defendant's Motion for Summary Judgment insofar as Defendant withheld the names and contact information of its individual employees who prepare or receive snapshots of the EID.

3. *Defendant's Segregability Analysis*

Plaintiffs also assert that Defendant did not perform a proper segregability analysis to ensure all non-exempt materials were released in response to their Third FOIA Request. Specifically, Plaintiff challenges whether Defendant met its obligations under FOIA because it has not provided a *Vaughn* Index or other description of the materials that contributed to or are excerpted in the Nine-Page Document. *See* Pls.' Suppl. Summ. J. Br. at 13–15. Defendant responds only that the existence of the Nine-Page Document is evidence that it performed a proper segregability analysis. *See* Defs.' Suppl. Reply Br. at 20. At this juncture, the court passes judgment only as to Defendant's withholdings under Exemption 6; whether Defendant properly segregated any materials potentially exempt under Exemption 7(C) or 7(E) from non-exempt material is an issue for another day. *Cf. Sussman*, 494 F.3d at 1116 (explaining that the district court must make a segregability finding if it approves a withholding).

The court is satisfied that Defendant segregated the names and contact information of federal employees before withholding that information under Exemption 6. The court begins from the presumption that Defendant complied with its statutory obligation, and Plaintiff has pointed to no evidence to the contrary. *Id.* at 1117. Although Defendant's conclusory explanation is certainly sub-par, the court's own review of the record leaves it confident that Defendant properly segregated the names and contact information of federal employees before redacting them from the Nine-Page Document. *See, e.g., Elec. Privacy Info. Ctr. v. Customs & Border Patrol*, No. 14-1217, 2017 WL 1131875, at \* 5 (D.D.C. Mar. 24, 2017). Indeed, Defendant's *Vaughn* Index specifically notes that it withheld, pursuant to Exemption 6, only "the names, phone numbers, and

email addresses of employees of law enforcement agencies who manage the various systems with which the [EID module] interacts.” *See Am. Vaughn Index*], at 10 (No. 14). Moreover, the Nine-Page Document itself off-sets as a category “Recipient/Technical POC” and redacts material under that header, with the phrase “(b)(6)” visible in the redaction and portions of a telephone number left in places. On this record, the court holds Defendant met its segregability obligation as to the withheld names and contact information of federal employees.

Accordingly, the court grants Defendant’s Motion for Summary Judgment and denies Plaintiffs’ Cross-Motion for Summary Judgment insofar as those motions relate to Defendant’s segregation of the exempt names and contact information of federal employees from other, potentially non-exempt material.

#### **IV. CONCLUSION AND ORDER**

In light of the foregoing, the court grants Defendant’s Motion for Summary Judgment and denies Plaintiffs’ Cross-Motion for Summary Judgment as to Defendant’s appropriate segregation and withholding of the names and contact information of employees who prepare and receive snapshots of the EID, but the court denies both Defendant’s Motion and Plaintiffs’ Cross-Motion in all other respects. After multiple rounds of supplemental briefing, the court believes continuing to litigate this case on paper regarding Defendant’s assertion of FOIA Exemptions 7(C) and 7(E) to withhold the EID and IIDS metadata and database schema and material responsive to Plaintiffs’ Third FOIA Request is no longer the most efficient means of resolving the parties’ dispute. An evidentiary hearing is necessary.

The court orders the parties to appear for a status hearing on October 12, 2017, at 11:00 a.m., in Courtroom 10, to discuss how an evidentiary hearing in this matter should proceed. The parties shall be prepared to discuss, among other things, how many witnesses they intend to call,

what documents they expect to introduce, and whether any records or testimony will need be taken under seal or ex parte.

Dated: September 29, 2017



Amit P. Mehta  
United States District Judge