UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

SUSAN B. LONG, et al.,	)	
Plaintiffs,	)	
v.	)	**Case No. 14-cv-00109 (APM)**
IMMIGRATION AND CUSTOMS ENFORCEMENT, et al.,	)	
Defendants.	)	

MEMORANDUM OPINION AND ORDER

I. INTRODUCTION

Plaintiffs Susan B. Long and David Burnham brought this action against Defendants Immigration and Customs Enforcement ("ICE") and Customs and Border Protection ("CBP") pursuant to the Freedom of Information Act ("FOIA") to challenge the agencies' responses to seven FOIA requests that Plaintiffs submitted between October 13, 2010, and February 26, 2013. In these requests, Plaintiffs sought a "complete set of documentation" on two databases used by both agencies as well as "snapshots" of data contained within one of the databases. Plaintiffs submitted the requests on behalf of the Transactional Records Access Clearinghouse at Syracuse University, which collects, organizes, and distributes data concerning federal government enforcement activities. In response to Plaintiffs' requests, Defendants produced some responsive documents but withheld or redacted many others, prompting this lawsuit.

After two rounds of summary judgment briefing, the court concluded that an evidentiary hearing was necessary to resolve two lingering issues related to ICE's invocation of Exemption 7(E) to withhold certain material responsive to Plaintiffs' first three FOIA requests—all of which were directed only to Defendant ICE ("Defendant" or "ICE").[1] Those issues are as follows: (1) whether ICE properly withheld metadata and database schemas in response to Plaintiffs' first two FOIA requests because disclosure could reasonably be expected to risk circumvention of the law; and (2) whether the materials or documents used to produce a summary document ICE prepared in response to Plaintiffs' third FOIA request were compiled for law enforcement purposes, and whether the release of the summary document in full could reasonably be expected to risk circumvention of the law.

Considering the evidence presented at the evidentiary hearing, as well as the arguments presented in the parties' briefs, supplemental memoranda, and at oral argument, the court concludes that, as to Plaintiffs' first and second FOIA requests, ICE reasonably concluded that comprehensive disclosure of all requested information could risk circumvention of the law. However, it appears that ICE may have withheld codes, code translations, field names, and table names that can reasonably be segregated from otherwise properly exempt materials. Therefore, the court orders ICE to conduct a segregability analysis as to these records. As to Plaintiffs' third FOIA request, ICE still has not provided any information indicating whether the underlying materials used to produce the summary document were compiled for law enforcement purposes. Accordingly, the court orders disclosure of that document in full, subject to the Exemption 6 withholdings the court previously approved.

II. BACKGROUND

The court has described the factual background and procedural history of this case at great length in previous memorandum opinions, *see Long v. ICE* (*Long I*), 149 F. Supp. 3d 39, 43–47 (D.D.C. 2015); *Long v. ICE* (*Long II*), 279 F. Supp. 3d 226, 230 (D.D.C. 2017), and need not

[1] The court previously granted summary judgment in favor of Defendant CBP on all issues pertaining to the requests directed to that agency. Thus, the court refers to ICE as the sole "Defendant" throughout this opinion.

repeat those details here. The court thus recites only what is necessary to resolve the remaining issues concerning Plaintiffs' first three FOIA requests, which survived summary judgment and formed the subject of the evidentiary hearing held on May 8 and 9, 2018.[2]

A. FOIA Requests I and II

In their first two FOIA requests, Plaintiffs sought "a complete set of documentation" on two databases owned and operated by ICE, which both ICE and CBP use to manage cases pertaining to the detention of undocumented immigrants: the Enforcement Integrated Database ("EID") and the Integrated Decision Support Database ("IIDS"). *Long I*, 149 F. Supp. 3d at 44–45; *see also* Defs.' Mot. for Summ. J., ECF No. 17 [hereinafter Defs.' Mot.], Ex. 1, ECF No. 17-3 [hereinafter FOIA Request I]; Defs.' Mot., Ex. 8, ECF No. 17-3 [hereinafter FOIA Request II].

1. FOIA Request I

Plaintiffs' first request, dated October 13, 2010, sought records related to the EID. *See* FOIA Request I. "The EID is the main repository of data for the enforcement of immigration law [by] ICE and CBP." 5/8/2018 Hr'g Tr., ECF No. 62 [hereinafter Day 1 Tr.], at 16:1-2. It "captures and maintains 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 and CBP. *Long I*, 149 F. Supp. 3d at 44 (quoting Defs.' Mot., Decl. of Karolyn Miller, ECF No. 17-1 [hereinafter Miller Decl.], ¶ 12); *accord* Day 1 Tr. at 16:5-13. The EID contains, among other things, "an array of personally identifiable information about persons detained for violating the Immigration and Nationality Act, including names, aliases, dates of birth, telephone numbers, addresses, Alien Registration Numbers, Social Security Numbers, passport numbers, and employment, educational, immigration, and criminal histories." *Long I*,

[2] For the sake of brevity, the court cites to its previous memorandum opinions as authority for stated facts that are either undisputed or immaterial for purposes of resolving the narrow issues that remain in the litigation.

149 F. Supp. 3d at 44 (citing Miller Decl. ¶ 12); *see* Day 1 Tr. at 16:5-11. It also contains information about arresting officers, the facility of detention for each immigrant taken into ICE's custody, and other investigative and sensitive law-enforcement information. *See* Day 1 Tr. at 16:11-13, 19:3-8; *see also* Sealed 5/8/2018 Hr'g Tr., ECF No. 58 [hereinafter Sealed Day 1 Tr.], at 119:1–120:9.

ICE uses the EID "to manage cases from the time of an undocumented immigrant's detention through the person's final case disposition." *Long I*, 149 F. Supp. 3d at 44 (citing Defs.' Mot., Decl. of Fernando Pineiro, ECF No. 17-2 [hereinafter Pineiro Decl.], ¶ 47). The EID is also used by other components within the Department of Homeland Security, such as the CBP and U.S. Citizenship and Immigration Services, as well as other federal agencies, such as the Department of State, the Federal Bureau of Investigation, and the Social Security Administration. *See* Day 1 Tr. at 16:14–18:6.

Plaintiffs' request for "a complete set of documentation on the [EID]" included:

> (1) a copy of the records identifying each and every database table in the EID and describing all fields of information that are stored in each of these tables. . . .
>
> (2) a copy of records defining each code used in recording data contained [in] the EID. This is a request for the contents of specific auxiliary tables—often referred to as code or lookup tables—within the database itself where this information is stored. . . .
>
> (3) a copy of the EID's database schema[,] [i.e.,] a specific class of records included in [the] database system that sets forth how the database tables are interlinked[;] [and]
>
> (4) records that identify the [Database Management System] software (e.g., Oracle, DB2, Sybase, SQL Server, etc.) including [the] Version No. used for the EID.

FOIA Request I at 1.

2. *FOIA Request II*

Plaintiffs' second request, dated October 18, 2010, sought the same information regarding the IIDS that the first request sought regarding the EID. *Long I*, 149 F. Supp. 3d at 44–45; *see* FOIA Request II. The IIDS is "a subset of the EID database repository . . . [that] provides a continuously updated snapshot of selected EID data." *Long I*, 149 F. Supp. 3d at 44 (alterations in original) (quoting Miller Decl. ¶ 13); *accord* Day 1 Tr. at 18:16-18. Its intended purpose is "to query EID data for operational or executive reporting purposes and is typically used to generate management reports and statistics from EID data." *Long I*, 149 F. Supp. 3d at 44–45 (quoting Miller Decl. ¶ 13); *see also* Day 1 Tr. at 18:13-18 (describing the IIDS as ICE's "reporting system"); *id.* at 19:11-24 (noting that the IIDS is used to produce regular reports on all enforcement actions as well as ad hoc reports for policymakers). Accordingly, the IIDS contains a subset of information from the EID "that can be counted statistically," Day 1 Tr. at 18:20-24, including "biographic information, information about encounters between agents/officers and subjects, and apprehension and detention information about all persons in EID," *Long I*, 149 F. Supp. 3d at 45 (quoting Miller Decl. ¶ 13). The IIDS is also used by ICE to respond to FOIA requests for certain data relating to its enforcement activities, including those submitted by the Transactional Records Access Clearinghouse, or "TRAC," on an ongoing basis. *See* Day 1 Tr. at 58:20-24; *see also Long v. Immigration & Customs Enf't*, No. 17-cv-01097 (APM), 2018 WL 4680278, at *2 n.4 (D.D.C. Sept. 28, 2018).[3]

In summary, Plaintiffs' first two FOIA requests sought records that (1) identified the names of EID and IIDS database tables and fields, (2) defined codes used to record data in those

[3] Plaintiffs' monthly requests for updated, anonymous, case-by-case information about persons removed as a result of one of ICE's immigration enforcement programs is the subject of another case currently pending before this court. *See Long v. Immigration & Customs Enf't*, No. 17-cv-1097 (D.D.C. filed June 8, 2017).

databases, (3) set forth the database schemas (that is, the way various database tables connect to each other), and (4) disclosed the particular software and version number used for the databases.

3. *ICE's Response to FOIA Requests I and II and the Parties' Motions for Summary Judgment*

In response to Plaintiffs' requests, ICE released 97 pages, with redactions, and withheld the remaining responsive information pursuant to FOIA Exemption 7(E),[4] which protects from disclosure "records or information compiled for law enforcement purposes" if their disclosure "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). In ruling on the parties' initial motions for summary judgment, the court held that the withheld material responsive to Plaintiffs' first two requests constituted records or information compiled for law enforcement purposes that qualified at least as law enforcement guidelines, if not also law enforcement methods and techniques. *See Long I*, 149 F. Supp. 3d at 48–50. The court also held that the claimed risk associated with disclosure of the EID and IIDS metadata and database schemas—the threat of a successful cyberattack on the databases—was "the kind of risk of circumvention of the law that justifies withholding" under Exemption 7(E). *Id.* at 51. Nevertheless, the court denied summary judgment, reasoning that it was unclear whether disclosure of the metadata and database schemas could reasonably be expected to risk circumvention of the law. *Id.* at 53–54. After giving ICE an opportunity to supplement the record and allowing the parties to renew their motions for summary judgment, the court reached the same

[4] The 97 redacted pages released by ICE were responsive only to Plaintiffs' second FOIA request, which sought records relating to the IIDS. *See* Pineiro Decl. ¶¶ 16–19. ICE did not produce *any* information in response to Plaintiffs' first FOIA request concerning the EID, on the grounds that "the release of any additional responsive records . . . would expose ICE's sensitive law enforcement data systems." *Id.* ¶ 15.

conclusion once more, holding that genuine disputes of material fact remained as to the reasonableness of ICE's expectation of risk. *See Long II*, 279 F. Supp. 3d at 238–39. The court concluded that an evidentiary hearing was required to resolve the parties' dispute. *Id.* at 245.

B. FOIA Request III

Plaintiffs' third FOIA request, dated September 21, 2012, sought information relating to "snapshots" and extracts of the EID over a 12-month period. *Long I*, 149 F. Supp. 3d at 45; *Long II*, 279 F. Supp. 3d at 230–31, 239. In particular, Plaintiffs requested records identifying (1) "extracts and 'snapshots' prepared from the [EID] over the last 12 months," along with records relating to (2) "the frequency with which such extracts and snapshots have been prepared"; (3) "who was responsible for preparing any snapshot or extract"; (4) "the recipient(s) of th[e] extracts/snapshots"; and (5) "the EID system time required in their preparation during this period." Defs.' Mot., Ex. 14, ECF No. 17-3 [hereinafter FOIA Request III]. In response to this request, ICE created a nine-page document ("the Nine-Page Document") summarizing the responsive materials and released a redacted version of that document. *Long II*, 279 F. Supp. 3d at 231; *see also* Pineiro Decl. ¶ 27. ICE did not, however, release the original responsive materials. *Long II*, 279 F. Supp. 3d at 231.

Of the five categories of materials sought in Plaintiffs' third FOIA request, *see id.* at 239, only the first, second, and fifth categories remain at issue, *see id.* at 241.[5] ICE withheld information responsive to these three categories—specifically, "the timing and frequency of snapshots, as well as the names of the law enforcement systems that interact with a particular EID module"—pursuant to Exemption 7(E). *See id.* at 241; *see also* Defs.' Suppl. Br. in Supp. of Defs.'

[5] The court granted summary judgment in favor of ICE with respect to its withholding of the third and fourth categories of information, i.e., the names, phone numbers, and email addresses of employees who manage the systems with which the EID module interacts, pursuant to Exemption 6. *See Long II*, 279 F. Supp. 3d at 243–45.

Mot. for Summ. J., ECF No. 35 [hereinafter Defs.' Suppl. Summ. J. Br.], at 18–20, 25–26; Notice of Suppl. Evidence, ECF No. 32, Suppl. Decl. of Jeff Wilson, ECF No. 32-2, ¶¶ 15–27, 44–49; Notice of Filing Suppl. Vaughn Index, ECF No. 24, Vaughn Index, ECF No. 24-2, at 10 (No. 14).

The court denied summary judgment on this issue because ICE failed to present 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," 5 U.S.C. § 552(b)(7). *See Long II*, 279 F. Supp. 3d at 241–43. Absent such evidence, the court explained, the court could not discern whether any portion of the Nine-Page Document was eligible to be withheld pursuant to FOIA Exemption 7. *Id.* at 243. Moreover, the court explained that even if it were to assume that the Nine-Page Document was created from materials compiled for law enforcement purposes, the court still would be unable to determine whether ICE properly invoked Exemption 7(E) to redact information relating to the timing and frequency of snapshots, as ICE relied on the same rationale that it did to withhold materials responsive to Plaintiffs' first two FOIA Requests. *Id.* at 243 n.8.[6] Accordingly, the court held that an evidentiary hearing was necessary to resolve this issue, as well. *See id.* at 245; *see also* 10/12/2017 Draft Hr'g Tr. at 14–15.

C. Evidentiary Hearing

On May 8 and 9, 2018, the court held an evidentiary hearing to resolve the parties' dispute related to the propriety of ICE's invocation of Exemption 7(E) to withhold EID and IIDS metadata and database schemas as well as certain material responsive to Plaintiffs' third FOIA request for information concerning EID extracts and snapshots. During the hearing, the court heard

[6] Because the court denied summary judgment as to the applicability of Exemption 7(E) to withhold the abovementioned portions of the Nine-Page Document, the court saved for another day the question whether ICE properly segregated any materials potentially exempt under Exemption 7(E) from non-exempt material. *Id.* at 244–45.

testimony—both in open court and in a sealed, ex parte session—from government witness Tadgh Smith, the Deputy Assistant Director for ICE's Law Enforcement Systems and Analysis Division ("LESA") of Enforcement Removal Operations. *See* 5/8/2018 Minute Entry. The court also heard testimony from two witnesses called by Plaintiffs: (1) Plaintiff Susan Long, who serves as a co-director of TRAC and who submitted the underlying requests at issue in this case, and (2) Dr. Paul Clark, who serves as the President and Chief Technology Officer of SecureMethods, Inc., and Paul C. Clark, LLC, and who Plaintiffs offered as an expert in computer security and design. *See id.*; 5/9/2018 Minute Entry.

Following the evidentiary hearing, each party submitted a supplemental memorandum, summarizing the evidence that supported their respective positions concerning the application of Exemption 7(E). *See generally* Def.'s Post-Evidentiary H'rg Suppl. Mem., ECF No. 60 [hereinafter Def.'s Suppl. Mem.]; Pls.' Post-Hr'g Suppl. Mem., ECF No. 61 [hereinafter Pls.' Suppl. Mem.]. The court held oral argument on these submissions on July 27, 2018. 7/27/2018 Minute Entry.[7]

III. LEGAL STANDARD

"The basic purpose of FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed." *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978). Because of FOIA's critical role in promoting transparency and accountability, "[a]t all times courts must bear in mind that FOIA mandates a 'strong presumption in favor of disclosure.'" *Nat'l Ass'n of Home Builders v. Norton*, 309 F.3d 26, 32 (D.C. Cir. 2002) (quoting *U.S. Dep't of State v. Ray*, 502 U.S.

[7] Some of the delay in resolving this matter is attributable to the parties' eight-month-long efforts to settle this matter and the related case, *Long v. Immigration & Customs Enf't*, No. 17-cv-1097, which concluded in late July 2019. *See* 17-cv-1097, Joint Status Report, ECF No. 30. Nevertheless, the court regrets the length of time it has taken to issue this decision.

164, 173 (1991)). FOIA requires federal agencies to release all agency records responsive to a request for production, *see* 5 U.S.C. § 552(a)(3)(A), unless the records fall within one of nine narrowly construed exemptions, *id.* § 552(b); *see Vaughn v. Rosen*, 484 F.2d 820, 823 (D.C. Cir. 1973). "The agency bears the burden of establishing that a claimed exemption applies." *Citizens for Responsibility & Ethics in Wash. v. U.S. Dep't of Justice* ("*CREW*"), 746 F.3d 1082, 1088 (D.C. Cir. 2014). Moreover, "even when an exemption applies, the agency is obligated to disclose 'any reasonably segregable portion of a record' after removing the exempt material and must note the 'amount of information deleted, and the exemption under which the deletion is made.'" *Bartko v. U.S. Dep't of Justice*, 898 F.3d 51, 62 (D.C. Cir. 2018) (cleaned up) (quoting 5 U.S.C. § 552(b)).

Although the vast majority of FOIA cases are appropriately resolved on motions for summary judgment, the D.C. Circuit has observed that summary judgment is "not always" proper in a FOIA case. *Brayton v. Office of the U.S. Trade Representative*, 641 F.3d 521, 527 (D.C. Cir. 2011). Summary judgment is inappropriate where "there is a conflict in the affidavits as to what adverse consequences will flow from" disclosure of the materials withheld by the agency. *Sears, Roebuck & Co. v. Gen. Servs. Admin.*, 553 F.2d 1378, 1382 (D.C. Cir. 1977); *see Gov't Accountability Project v. FDA*, 206 F. Supp. 3d 420, 430 (D.D.C. 2016) (noting that while courts "routinely resolve FOIA disputes in the summary judgment context," summary judgment cannot be granted "if dueling affidavits create a genuine dispute over issues of material fact"). "Resolving issues of material fact in FOIA cases has, for example, required a bench trial to determine the propriety of exempting certain documents from release under the FOIA, or an evidentiary hearing." *Scudder v. CIA*, 25 F. Supp. 3d 19, 29 (D.D.C. 2014) (internal citation omitted).

Because evidentiary hearings are rare in the FOIA context, the case law outlining the standards that govern those proceedings is unsurprisingly thin. Nevertheless, the court agrees with Plaintiffs that "in those rare cases where, as here, facts bearing on exemption are genuinely disputed, the agency's burden requires it to prove by a preponderance of the evidence that the factual dispute should be resolved in its favor." Pls.' Suppl. Mem. at 13–14;[8] *cf. Nat'l Parks & Conservation Ass'n v. Kleppe*, 547 F.2d 673, 679–83 (D.C. Cir. 1976) (reviewing for clear error a trial court's findings—following a two-day evidentiary hearing—that certain factual predicates for an agency's withholding under Exemption 4 were supported by "[t]he preponderance of the evidence").

IV. DISCUSSION[9]

A. FOIA Requests I–II: EID and IIDS Metadata and Database Schemas

The court begins by determining whether ICE properly withheld EID and IIDS metadata and database schemas under Exemption 7(E) in response to Plaintiffs' requests for complete documentation of the EID and IIDS, respectively. Due to the technical nature of these requests, the court starts with the basics, providing a brief summation of the specific types of records requested by Plaintiffs before turning to ICE's justification for withholding the metadata and database schemas.

[8] While ICE's post-hearing supplemental memorandum does not outline a particular standard to be applied, *see* Def.'s Suppl. Mem., the agency did not take issue with the standard proposed by Plaintiffs, or advocate any other standard that should apply, at oral argument, *see* 7/27/2018 Draft Hr'g Tr.

[9] The court treats the Discussion section as the required findings of fact and conclusions of law under Federal Rule of Civil Procedure 52(a). *Cf. Kleppe*, 547 F.2d at 679 (reviewing a district court's findings following a FOIA evidentiary hearing under the standards set forth in Rule 52(a)). The court's factual findings are not set forth in a separate section in the opinion, as the parties' remaining dispute by and large concerns the inferences of risk that can be drawn from otherwise undisputed facts.

1. *Nature of the Information Requested*

As discussed, Plaintiffs' first two FOIA requests seek a complete set of documentation for the EID and IIDS databases, including: (1) a copy of records identifying the database tables and describing all fields of information stored within those tables; (2) a copy of records defining each code used to record data in the database, including the contents of any "code or lookup tables" in the databases; (3) a copy of the database schemas, i.e., the records in database systems that set forth how tables are interlinked; and (4) records identifying the Database Management System software and version number used for the databases. At this juncture, only the first three categories of records remain in dispute.[10]

a. Database tables and fields

Information within a database is organized into database "tables," which contain data on a particular subject. Day 1 Tr. at 136:12-21; *accord* Miller Decl. ¶¶ 7–8. The database tables can be analogized to the Excel spreadsheets that ICE typically uses to produce information from the databases. *See* Day 1 Tr. at 136:12-14; Miller Decl. ¶ 8; *cf.* Day 1 Tr. at 58:20–59:2, 71:7-16, 74:12-19. The tables typically comprise multiple "fields" of data, which correspond to columns in a spreadsheet. *See* Day 1 Tr. at 53:19-22, 59:3-16, 63:1-6, 73:2-13, 74:15–75:9, 98:2-23, 136:22-25, 170:12-16; 5/9/2018 Hr'g Tr., ECF No. 57 [hereinafter Day 2 Tr.], at 53:5–17; *see also* Miller Decl. ¶ 8. Rows within each table are the equivalent of a single record, which is a collection of information about a specific person or event (depending on the topic around which the table is organized). Miller Decl. ¶ 8; *accord* Day 1 Tr. at 136:16-25. "For example, in a table concerning

[10] Plaintiffs no longer contest ICE's response to their request for database management system software and version numbers. *See* Day 1 Tr. at 135:18-20 (testimony of Plaintiff Susan Long, stating that Plaintiffs' first two requests "singled out four specific classes [of information], one of which [ICE] provided . . . the database system[s] being used . . . they've provided that"); *see also* Pls.' Suppl. Mem. at 10 n.1.

immigration detainers, each row might represent a different detainer, and one field—that is, column—might record the date on which the detainer was lifted." Pls.' Suppl. Mem. at 3 (citing Day 1 Tr. at 77 and Pls.' Evidentiary Hr'g Ex. II, col. I).

Each table and field in the databases has a distinctive name. *See, e.g.*, Pls.' Evidentiary Hr'g Ex. AA (listing table name, as well as field names within each table, for two other EID modules); Pls.' Evidentiary Hr'g Ex. DDD at 37–97 (graphical depiction of table names and field names within IIDS);[11] *see also* Day 2 Tr. at 5:7–7:17. There are hundreds of database tables and thousands of fields within those tables. Day 1 Tr. at 20:21–21:6. Because the IIDS is a subset of the EID, the IIDS has its own set of table and field names, only some of which correspond with the EID table and field names. *See* Day 2 Tr. at 5:15–7:5; *see also* Pls.' Evidentiary Hr'g Ex. II.

b. Codes and code lookup tables

While some data entered into EID and IIDS fields take the form of intelligible English words or phrases or numerical values, data are often recorded in the form of codes. *See* Day 1 Tr. at 137:16-23; *see also* Miller Decl. ¶ 10 (explaining that codes are used to save space and reduce the size of records in a database); *cf.* Day 1 Tr. at 21:7–22:9. Codes are strings of alphanumeric characters that uniquely identify different pieces of information that may be recorded within a given field. *See* Day 1 Tr. at 63:13-20, 137:16–138:2. For example, the database might assign a unique numerical code for a particular county or detention facility, or a unique alphabetic code for a particular state, rather than spelling out the name of the county, facility, or state. *See id.* at 138:4-12. The databases also contain auxiliary tables, known as "code lookup tables," which provide a translation of the codes. *See id.* at 63:25–64:17, 66:21–67:7, 135:18–136:3, 138:3-25; *see, e.g.*, Pls.' Evidentiary Hr'g Exs. BB, DD.

[11] Citations to Plaintiffs' Exhibit DDD are to the page numbers of the PDF document.

c. Database schemas

A database schema provides "the blueprint of [a] database[]," laying out "exactly where everything is" in each database and "how it's stored." Day 1 Tr. at 23:5-22. It contains tables often referred to as data "dictionaries"—database tables that set forth the names of tables and fields within those databases. *See id.* at 23:2-12, 52:14–54:14; *see, e.g.*, Pls.' Evidentiary Hr'g Ex. AA (sheet four); *cf.* Day 1 Tr. at 137:1-13, 144:16–147:19. It also includes graphical depictions of the structure of the database, which includes not only the names of tables and fields therein, but also the ways in which the tables are connected to one another. *See* Day 1 Tr. at 23:7-22, 57:8-24. In the graphical depiction of the schema, each block represents a table, the items listed within each block represent field names with a table, and arrows between the blocks represent "linkages" between tables within the database. *See* Day 1 Tr. at 57:25–58:8, 157:6-9; *see, e.g.*, Pls.' Evidentiary Hr'g Ex. DDD at 31–97.

2. ICE's Justification for Withholding Responsive Material

With this context in mind, the court turns to ICE's justification for withholding EID and IIDS metadata and database schemas pursuant to Exemption 7(E). As discussed, the primary question before the court is whether the disclosure of such material "could *reasonably* be expected to risk circumvention of the law" under Exemption 7(E), 5 U.S.C. § 552(b)(7)(E) (emphasis added). To satisfy this requirement, an agency need only "demonstrate logically how the release of the requested information might create a risk of circumvention of the law." *Shapiro v. U.S. Dep't of Justice* (*Shapiro I*), 893 F.3d 796, 800 (D.C. Cir. 2018) (cleaned up) (quoting *Mayer Brown LLP v. IRS*, 562 F.3d 1190, 1194 (D.C. Cir. 2009)). "This is 'a relatively low bar.'" *Id.* (quoting *Blackwell v. FBI*, 646 F.3d 37, 42 (D.C. Cir. 2011)). Courts "generally have affirmed the withholding of information related to databases—metadata, codes, and structures—under

Exemption 7(E) for risk of cyber-attack or data breach." *Shapiro v. Dep't of Justice* (*Shapiro II*), 393 F. Supp. 3d 111, 122 (D.D.C. 2019) (collecting cases); *see also Levinthal v. Fed. Election Comm'n*, 219 F. Supp. 3d 1, 8 (D.D.C. 2016) ("[C]ourts in this District repeatedly have held that information connected to law enforcement databases qualifies for exemption under 7(E).").

Even when an exemption broadly applies, however, an agency nevertheless must "tailor" its withholdings to only that which the exemption protects. *Inst. for Justice v. IRS*, 941 F.3d 567, 574 (D.C. Cir. 2019). Thus, the agency must "account for its obligation to disclose any reasonably segregable portion of a record after removing the exempt material." *Id.* (cleaned up).

a. Risk of Circumvention

The primary risk of circumvention of the law identified by ICE is the danger that a hacker with access to the requested information will be able to carry out a more efficient and effective cyberattack against the EID and IIDS databases. According to ICE, this risk flows from the disclosure of EID and IIDS metadata and database schemas because hackers with advance knowledge of such information would be able to "set up their own version of the database and practice attacks in isolation, where they can't be witnessed and [can] perfect their attack." Defs.' Suppl. Mem. at 4 (quoting Day 1 Tr. at 35:9-13). The agency's witness, Tadgh Smith, testified that "if you already know how [a database is] organized, you can make your attack very targeted, . . . less likely to be noticed," or even "cover up [your] tracks that [you] attacked [the database] in the first place." Day 1 Tr. at 45:9-13.

According to Smith, this advance knowledge would aid an attacker in executing a Structured Query Language ("SQL")[12] injection attack on the EID and IIDS databases, *see* Day 1 Tr. at 47:18-23.

[12] SQL is a programming language that is used to access and manipulate records within a database. *See* Miller Decl. ¶ 16.

> The SQL injection attack . . . is a technique used by malicious intruders or "hacktivists" to exploit web sites by changing the intended effect of an SQL query by inserting new SQL keywords or operators into the query. Basically, the attacker inserts or 'injects' SQL instructions in a web application Search field to cause the program to malfunction.

Long I, 149 F. Supp. 3d at 50–51 (quoting Miller Decl. ¶ 16); *accord* Day 1 Tr. at 47:5-13 (Smith Testimony); Day 2 Tr. at 90:3-19 (Clark testimony). Once a hacker gains a direct connection to the database, he can issue "ad hoc commands" for the purpose of "corrupting the database in some way," Day 2 Tr. at 90:13-18, allowing him to "change" or "delete" data, or "merely read data [that he is] not supposed to see," Day 1 Tr. at 47:14-17; *see also* Day 2 Tr. at 90:19. Smith testified that the information requested by Plaintiffs could be used in an SQL attack because a person who knows the organization of a database will "know how to query that database" and, further, a person who knows the table and field names in a database will be able to "target [their] attack." Day 1 Tr. at 47:22–48:1. Smith suggested that these types of attacks may be executed not only by outside bad actors, but also rogue insiders who would not otherwise have access to the databases. *See id.* at 44:15–48:1.

At the evidentiary hearing, ICE—for the first time in four years of litigation—presented testimony concerning remote access to the EID and IIDS, *see id.* at 26:11–29:2, a material fact that has been a point of contention throughout this litigation, *see Long II*, 279 F. Supp. 3d at 236 (noting that "it remains ambiguous to the court whether the [databases] can be externally or remotely accessed," and that this question is "material" because "Defendant's argument centers on the fact that a circumvention of law occurs only when a hacker *accesses* the database[s]"). In light of this testimony, the court is satisfied that the databases are remotely, albeit not publicly, accessible via a trusted internet connection, or "TIC," and the parties do not seriously dispute this fact. *See* Def.'s Suppl. Mem. at 3; *cf.* Pls.' Suppl. Mem. at 10. This means that the execution of the aforementioned attack is possible, provided that the attacker manages to gain access to the databases by subverting the TIC, *see* Day 1 Tr. at 25:17–26:25, 32:5-9, and additional layers of security, *see id.* at 87:24–88:11.

ICE asserts that advance knowledge of the metadata and database schemas would provide the malicious intruder who manages to gain access to the databases (by circumventing the TIC and other layers of protection) with the means to create greater mischief once inside. *See* Def.'s Suppl. Mem. at 3–5. In other words, the asserted risk is tied to the *additional* damage a hacker might cause once he gains unauthorized access to the EID and IIDS if he has advance knowledge of the metadata and database schemas—not the prospect that he will gain such access in the first place by successfully managing to subvert the TIC and traverse any security measures intended to protect those databases. In this case, that additional harm might consist of viewing, modifying, or deleting sensitive law enforcement information related to ICE's enforcement duties,[13] and possibly even erasing any evidence that the databases were attacked or otherwise compromised. *See* Day 1 Tr. at 44:23–45:13; 47:2–48:1; *see also* Sealed Day 1 Tr. at 116:21–117:8.

Plaintiffs attack ICE's risk assessment on two grounds. First, they maintain that, notwithstanding ICE's new evidence concerning access to the databases via the TIC, the security measures employed by ICE to protect its databases are adequate to restrict unauthorized access, and so any additional protections provided by the non-disclosure of the metadata and schemas would be superfluous. *See* Pls.' Suppl. Mem. at 10–11. Second, they contend that even if a would-be attacker were to gain access to the databases, advance knowledge of the metadata and database schemas would not materially aid the attacker in doing any damage. *Id.* at 1, 11–12.

[13] ICE's witness explained in further detail the sensitivity of the information contained within the EID and IIDS databases in testimony during the sealed portion of the hearing. *See* Sealed Day 1 Tr. at 118:19–120:9.

Plaintiffs' first argument is easily dismissed. While the evidence adduced at the evidentiary hearing demonstrates that there are security countermeasures in place to prevent a hacker from gaining access to the system, *see* Day 1 Tr. at 29:3-5, 105:14-25, 107:19–109:2 (Smith testimony); Day 2 Tr. at 77:8-13, 78:2–90:2, 93:25–97:12, 100:4-12 (Clark testimony), nowhere was it credibly suggested that access is impossible. Indeed, based on the testimony presented during the sealed, ex parte portion of the proceedings, the court finds that ICE's systems are not impervious to breach. *See* Sealed Day 1 Tr. at 115:6-14, 116:9-20.

Furthermore, the court finds that Dr. Clark's opinion that an external breach of ICE's security measures is unlikely was heavily based on his erroneous assessment that the EID and IIDS are not "particularly high-value assets" from an attacker's perspective. *See* Day 2 Tr. at 94:11-12, 126:12-13. Dr. Clark, however, acknowledged that he was "not familiar with the data structures in the database," *id.* at 126:17-21, and he admitted that he was unaware that the databases include highly sensitive categories of law enforcement information, *see id.* at 126:17–129:5—a fact which was described to the court in detail during the sealed portion of the evidentiary hearing, *see* Sealed Day 1 Tr. at 119:1–120:9 (Smith testimony). Dr. Clark's risk assessment was therefore inevitably deflated by that undervaluation. Additionally, notwithstanding Dr. Clark's expertise in computer network security and design, the court must afford some deference to Smith's testimony in this context, as his assessment of the risks of breach "reflects [his] access to more information than is available to either" Plaintiffs, Dr. Clark, or this court. *Sheridan v. U.S. Office of Pers. Mgmt.*, 278 F. Supp. 3d 11, 25 (D.D.C. 2017); *see also Long I*, 149 F. Supp. 3d at 53 ("Judges are not cyber specialists, and it would be the height of judicial irresponsibility for a court to blithely disregard such a claimed risk."). The court therefore finds that there is a sufficient risk that an attacker could gain access to ICE's databases, such that any additional protections afforded by the non-disclosure of the requested information would not be superfluous.

While Plaintiffs' second argument is a closer call, the court finds that it is not unreasonable for ICE to expect that greater harm might result from a cyberattack where the attacker has detailed advance knowledge of the structure and organization of the databases. A hypothetical is instructive here. Imagine a pair of art thieves who are planning to steal a valuable piece of artwork believed to be located in a museum's non-public storage vaults. The thieves have acquired a map of a museum that provides no information about how to get inside, but identifies the location of the museum's motion sensors and the layout of the vaults. The map would, of course, offer the art-loving larcenists no help in distracting the guards stationed outside or in picking the museum's locks. But, by memorizing its contents, the thieves might enjoy more success once inside, potentially avoiding otherwise invisible motion sensors and moving more efficiently through the non-public areas of the building. With the benefit of the map, the thieves might avoid detection entirely, or at the very least, avoid apprehension by pulling off the heist more quickly.

Here, the database schemas and at least some of the other metadata that Plaintiffs seek are like the thieves' map. The database schemas in particular are "blueprint[s] of the databases" that "lay[] out exactly where everything is and how it's stored." Day 1 Tr. at 23:20-22. Smith credibly testified that advance knowledge of this information would assist a hacker in launching a more targeted and effective attack that is less likely to be detected by the agency. *See* Day 1 Tr. at 35:5-13, 45:5-11, 47:2–48:1. Plaintiffs' own expert witness, Dr. Clark, acknowledged that advance knowledge of the metadata and database schemas could make *some* difference in an attack by enabling an attacker to recreate the database to practice his attack. Day 2 Tr. at 134:4-11. This advance knowledge, Dr. Clark conceded, could reduce the number of queries necessary for a hacker to accomplish his attack, thereby making the attack more efficient. *See id.* at 135:15-19 (acknowledging that a hacker's advance "ability to list the contents of the database prior to [his attack]" would lead to a "difference in time" required for the hack); *id.* at 136:14 ("There would be a delta [in time] . . . .").

Though Dr. Clark opined that this "delta" of time "would be small," *see, e.g.*, *id.* at 136:8-14, and "it would be a matter of a couple queries," *id.* at 135:18-19, the court finds the difference in time to be sufficient to satisfy Exemption 7(E)'s low bar, particularly given the highly sensitive nature of the law enforcement information contained in the databases. "[I]t is by now well established that an agency that invokes Exemption 7(E) need not show that an identified risk will actually increase substantially, or that the risks it relies upon will necessarily come to fruition." *Sheridan*, 278 F. Supp. 3d at 25. Instead, "exemption 7(E) only requires that the agency demonstrate *logically* how the release of the requested information *might* create a risk of circumvention of the law." *Id.* (cleaned up) (quoting *Mayer Brown LLP*, 562 F.3d at 1194). True, the disclosure of the metadata and database schemas in this case would not *directly* enable a cyber-attack. *See Long I*, 149 F. Supp. 3d at 51 (noting the "the potential for a cyber-attack . . . is the kind of risk of circumvention of the law that justifies withholding under Exemption 7"). But, by enabling a hacker to move faster through the databases to view, modify, or delete data, disclosure of the requested information could incentivize future attacks and make those attacks more harmful. This increased risk of harm is well within the scope of FOIA's Exemption 7(E). *See Shapiro II*, 393 F. Supp. 3d at 122 (upholding an agency's withholding of a database name based on the agency's representation "that knowledge of the 'database name[] makes the original source data an attractive target for compromise'"); *Strunk v. U.S. Dep't of State*, 905 F. Supp. 2d 142, 147 (D.D.C. 2012) (finding that an agency permissibly withheld sensitive database codes based in part on the agency's contention that "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" the database and would "arm unauthorized users with the ability to corrupt the integrity of the data contained therein"); *cf. Mayer Brown*, 562 F.3d at 1193 (holding that the IRS properly withheld certain settlement guidelines pursuant to Exemption 7(E) on the ground that those guidelines "could *encourage* decisions to violate the law or evade punishment," even if they didn't "necessarily provide a blueprint for tax shelter schemes" (emphasis added)).

Furthermore, a faster attack is not the only risk associated with the information Plaintiffs seek. Smith also testified that advance knowledge of the databases' organization could enable attackers to "cover up their tracks," making it "less likely" that the attack would "be noticed, monitored or even discovered." Day 1 Tr. at 45:10-12. Dr. Clark did not address this distinct threat during his testimony. Plaintiffs also ignore this risk in their supplemental briefing, contending only that advance knowledge of the databases' organization and structure would not provide an attacker a meaningful "head start." *See* Pls.' Suppl. Mem. at 11–12. Based on Smith's uncontroverted testimony, particularly that given during the sealed portion of the hearing, *see* Sealed Day 1 Tr. at 116:15–117:18, the court finds that there is a material risk that comprehensive knowledge of the organization of the databases could enable a bad actor to execute an attack undetected. FOIA Exemption 7(E) does not countenance such risk. *See Prechtel v. Fed. Commc'ns Comm'n*, 330 F. Supp. 3d 320, 335 (D.D.C. 2018) (holding that an agency appropriately withheld electronic server logs whose release would give "future attackers a 'roadmap' to evade the [agency's] future defensive efforts"); *Sheridan*, 278 F. Supp. 3d at 25 (concluding that an agency permissibly withheld source code that would "identify the 'locked doors' that have been designed into [its] software (telling a malicious actor where and how to attempt to breach [the] system)").

In sum, while the risk of conferring any material advantage on future hackers by disclosing the full suite of metadata and database schemas may not be imminent or severe, the court cannot conclude that it is *unreasonable* to expect that such a risk might come to fruition in light of Smith's testimony.[14]

b. ICE's Segregability Analysis

That does not end the analysis, however. Even when a FOIA exemption applies, "[a]ny reasonably segregable portion of a record shall be provided . . . after deletion of the portions which are exempt." 5 U.S.C. § 552(b). "Before approving the application of a FOIA exemption, the district court must make specific findings of segregability regarding the documents to be withheld." *Sussman v. U.S. Marshals Serv.*, 494 F.3d 1106, 1116 (D.C. Cir. 2007). Indeed, the court must make such a finding "even if the requester did not raise the issue of segregability before the court." *Id.*

Several factors suggest that ICE may have withheld segregable, non-exempt materials. Most importantly, Smith acknowledged at the evidentiary hearing that the disclosure of certain information sought by Plaintiffs would not create any additional risk to the security of ICE's databases. For example, Smith testified that the codes and code translations within certain code

[14] Smith also opined the disclosure of the database metadata and schema could present a risk of a "phishing" attack, where a bad actor could use knowledge of the "setup of the system" to trick an ICE employee into clicking on a malicious link or otherwise following an "instruction that will be beneficial to the attacker." Day 1 Tr. 48:2-23; *see also* Def.'s Suppl. Mem. at 5. The court does not address this threat because it appears that the risks associated with a phishing attack versus an SQL attack are similar. To the extent the risks are not coextensive, however, the court rejects Defendant's argument that the danger of phishing provides an independent basis for its withholdings. The "key" reason, according to ICE, that the withheld information presents a risk of a phishing attack is that it is not "publicly available information." 7/27/2018 Draft Hr'g Tr. at 9. But that argument is circular. The information is not publicly available only if it is subject to one of FOIA's nine exemptions. ICE has identified nothing unique about the withheld information that would create more of a risk of phishing than any other otherwise non-publicly available information that is subject to FOIA.

lookup tables could be released without creating an unacceptable threat to the security of the EID and IIDS databases, *see* Day 1 Tr. at 66:24–67:10, and that any other metadata contained within the tables that might pose a risk could be easily redacted, *see id.* at 70:9–71:6. Similarly, Smith testified that not all field names pose the same risk, if released. While Smith explained that ICE tries to replace actual field names with a plain-language description in its reporting and its responses to FOIA requests, *id.* at 40:25–41:19, he acknowledged that the disclosure of actual field names will not always create an independent threat to the security of the databases, *see, e.g.*, *id.* at 41:20–42:5. Instead, Smith explained that the "sensitive" field names are those that could indicate, "through coding best practice," how the databases are connected to one another, allowing a hacker to "reverse engineer" the database schema in order to rebuild the database. *Id.* at 42:6–43:25. As with the other metadata contained within the code lookup tables, Smith testified that if ICE were to produce to Plaintiffs an Excel spreadsheet that contained those field names that show linkages between multiple database tables, the agency could redact those field names while still producing others. *See id.* at 71:7-12.

While Smith later suggested that, under ICE's "defense in depth" security protocol,[15] disclosing *any* of the information requested by Plaintiffs would create an unacceptable risk, *id.* at 112:23–113:1, the court cannot square this statement with Smith's earlier testimony. Nor can the court accept the agency's invitation to rely on ICE's policy of defense in depth as an independent basis to withhold the information requested here. Doing so would afford blanket protection to every detail about the agency's databases, without further explanation or justification. *See id.* at 112:25–113:8 (opining that "there's a threat at every layer with every detail that's released"); *see also* 7/27/2018 Draft Hr'g Tr. at 15 (stating that "Mr. Smith explained during his testimony . . .

[15] Defense in depth is a cybersecurity protocol in which multiple, iterative layers of countermeasures are used to secure a network system. *See* Day 1 Tr. at 29:6–30:13; Day 2 Tr. at 91:7-12.

that really any little piece of information that is out there could lead to potential harm"). The court need not decide whether "defense in depth" is an outdated approach to cybersecurity, as Plaintiffs' expert suggests, *see* Day 2 Tr. at 91:7–92:7, 97:13–98:24; even if it remains an accepted security practice, its mandate of virtually limitless non-disclosure is incompatible with FOIA.

In addition, ICE recently publicly disclosed some of the metadata at issue in this case, suggesting that it has withheld segregable, non-exempt information and undermining its contention that "defense in depth" requires non-disclosure of any and all database details. While the court is satisfied that ICE's disclosures of the EID and IIDS database schema and metadata in 2010 and 2011 were inadvertent,[16] ICE's contemporaneous disclosures of subsets of these data lack such an explanation. For instance, Dr. Long testified, and ICE did not dispute that, in the two weeks prior to the evidentiary hearing, ICE produced to TRAC field names, codes, code translations, and code lookup tables from portions of the EID and IIDS databases. *See* Day 1 Tr. at 179:3-11; *id.* at 143:2–144:14. In addition, in November 2017, in response to a lawsuit filed by Plaintiffs against ICE in the Southern District of New York, ICE filed a declaration that provided "data points" (including field names) that "exist[] within IIDS" and identified several dozen such fields by their actual EID names. *See* Decl. of Marla Jones, ECF No. 15-1, at 7–10 *Long v. ICE*, 5:17-cv-00506-BKS-TWD (S.D.N.Y Nov. 8, 2017); *see also* Pls.' Suppl. Mem. at 6–7. ICE simultaneously filed two spreadsheets of responsive information, which apparently included code translations and IIDS field names with the underbars replaced by spaces. *See* Pls.' Suppl. Mem. at 7; *see also* Pls. Evidentiary Hr. Exs. YY, ZZ; Day 2 Tr. at 14:19–16:23.

[16] Smith testified that these disclosures were mistaken, that the agency has since taken steps to update its FOIA protocol and mitigate the security threat caused by the releases, and that the databases themselves have been substantially updated since the releases. *See* Day 1 Tr. at 36:14–40:4; *see also id.* at 159:1-6 (Long testimony, acknowledging that the 2010 and 2011 releases "would not necessarily at all reflect all of the fields that might [currently] be in the database"). Given these developments, the court finds that these particular disclosures do not have any bearing on the reasonableness of ICE's withholdings under Exemption 7(E) or the adequacy of the agency's segregability analysis.

Given Smith's admissions and ICE's contemporaneous disclosures of codes, code translations, and field names (both actual names and thinly disguised substitutes), the court cannot conclude that ICE has released all reasonably segregable material. As best the court can discern, only metadata that "describes the organization of [ICE's] data and the structure of [its] databases," presents any risk, *see* Day 1 Tr. 62:21-22, and it appears that only such metadata that cannot be readily intuited from other contexts presents a material risk, *see id.* at 41:20–42:5 (Smith opining that there would be no danger in releasing the field name "AD" (a code for Address) "because it's pretty easy to figure out that the content of that field is something we would release and that an abbreviation could be extrapolated out to that language"). The court is satisfied that the database schemas (which, by definition, describe the structure of ICE's databases) present such a material risk. But the other categories of information requested by Plaintiffs—field and table names, codes, code translations, and code lookup tables—do not appear to uniformly pose such a risk.[17]

Therefore, the court upholds ICE's withholdings as to the database schemas and directs ICE to conduct a segregability analysis as to the additional requested metadata.

B. FOIA Request III: Records Concerning EID Extracts and Snapshots

Next, the court turns to ICE's withholding of certain information relating to EID extracts and snapshots in response to Plaintiffs' third FOIA request. Recall that the court previously denied summary judgment on this issue because ICE had failed to present 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. *See Long II*, 279 F. Supp. 3d at 241–43. "In the absence of any" such evidence, the court explained, it could not "discern if

[17] It is possible that the segregation of a dataset this large would not be "reasonabl[e]," *see* 5 U.S.C. § 552(b), or that the disclosure of all non-structural metadata would nevertheless reveal too much about the databases' structure. ICE has not made any such representation, however.

any portion of the Nine–Page Document is eligible to be withheld pursuant to FOIA Exemption 7." *Id.* at 243.[18]

The court has reminded ICE of the need for this information multiple times. At the evidentiary hearing, for instance, the court instructed ICE that it had not "heard anything about" the Nine-Page Document "in terms of the source material for this information and whether it would qualify as law-enforcement material," Day 1 Tr. at 126:17-19, and that "in order to even meet the threshold for 7(E), there needs to be some evidence that the underlying material upon which this document was drawn itself is . . . compiled for law-enforcement purposes," *id.* at 127:6-10; *see also* 10/12/2017 Draft Hr'g Tr. at 6, 14–15 (discussing the need for additional information on this issue). ICE responded that it intended to provide this information "by way of a supplemental affidavit." Day 1 Tr. at 129:10-12.

At the oral argument held following the evidentiary hearing, the court reiterated that it had not received any evidence regarding whether the information underlying the Nine-Page Document had been compiled for law enforcement purposes, and ICE again indicated that its "intention [was] to submit a declaration concerning the nine page document." 7/27/2018 Draft Hr'g Tr. at 21–23. The court stressed that "there have been a number of mile posts in this case where evidence could have been and should have been submitted," and that it was not the court's intention to leave the record open "beyond the opportunity that was given at the end of the hearing to receive additional evidence" on the sources of the Nine-Page Document. *Id.* at 41.

ICE never submitted the promised declaration, and the court continues to be unable to "discern what materials contributed to the Nine–Page Document and, correlatively, whether those materials were compiled for law enforcement purposes." *Long II*, 279 F. Supp. 3d at 242.

[18] The court held, however, that Defendants properly withheld under Exemption 6 the names and contact information of the federal employees identified in the Nine-Page Document. *Id.* at 244.

Consequently, it remains unclear whether "any portion of the Nine-Page Document is eligible to be withheld pursuant to FOIA Exemption 7." *Id.* at 243.[19] The agency now has had multiple bites at the apple, and still has not met its "burden of establishing that a claimed exemption applies." *CREW*, 746 F.3d at 1088. Accordingly, the court orders disclosure of the Nine-Page Document in full, excepting the information it properly withheld pursuant to FOIA Exemption 6. *See Long II*, 279 F. Supp. 3d at 243–44.

V. CONCLUSION AND ORDER

For the reasons set forth above, the court orders the following:

1. As to Plaintiffs' first and second FOIA requests, ICE permissibly concluded that comprehensive release of this information is reasonably expected to risk circumvention of the law. As to the requested field and table names, codes, code translations, and code lookup tables, however, ICE must conduct a segregability analysis consistent with this opinion. In particular, ICE should evaluate whether the requested metadata that does not link to other portions of the databases or otherwise reveal the databases' structure can be released, and whether linkage fields and other sensitive data can be redacted. ICE need not conduct an additional segregability analysis as to the database schemas, however.
2. As to Plaintiffs' third FOIA request, ICE must disclose the Nine-Page Document in full, subject to the Exemption 6 redactions that the court has previously upheld.

[19] Because ICE has not met its burden as to this threshold question, the court does not reach the separate question of "whether there is a reasonable risk of circumvention of law from the disclosure" of the withheld portions of the Nine-Page Document. *See Long II*, 279 F. Supp. 3d at 243 n.8.

3. ICE shall submit its supplemental segregability analysis no later than July 2, 2020. The parties shall also file a Joint Status Report on the same day, regarding ICE's disclosure of the Nine-Page Document and any other outstanding issues in this litigation.

Amit Mehta

Dated: June 2, 2020

Amit P. Mehta
United States District Judge