UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Susan B. Long, *et al.*,

Plaintiffs,

v. | **Civil No. 14-00109 (APM)**

Immigration and Customs Enforcement, *et al.*,

Defendants.

MEMORANDUM OPINION AND ORDER

I. INTRODUCTION

Plaintiffs Susan B. Long and David Burnham bring this suit under the Freedom of Information Act ("FOIA"). Between October 13, 2010, and February 26, 2013, Plaintiffs submitted seven FOIA requests to two federal agencies, Defendant Immigration and Customs Enforcement and Defendant Customs and Border Patrol. They sought metadata and database schema from databases used by both agencies, as well as "snapshots" of data contained within one of the databases. Defendants produced some documents in response. But they withheld a host of others, relying on FOIA Exemptions 3 and 7 and claiming that producing certain responsive materials would be overly burdensome. Plaintiffs brought this suit claiming that Defendants violated FOIA by failing to provide them with all materials responsive to their requests.

Upon consideration of the parties' submissions and the record evidence, the court grants in part and denies in part the parties' Cross-Motions for Summary Judgment.

II. BACKGROUND

Plaintiffs Susan B. Long and David Burnham are Co-Directors of the Transactional Records Access Clearinghouse ("TRAC"), "a research center established by Syracuse University that gathers information about the functioning of federal law enforcement and regulatory agencies, analyzes the data, and publishes reports." *See* Pls.' Mot. Summ. J., ECF No. 18 [hereinafter Pls.' Mot.], Decl. of Susan B. Long, ECF No. 18-2 [hereinafter Long Decl.], ¶ 2. TRAC's primary purpose is "to provide comprehensive information about the staffing, spending, and enforcement activities of the federal government." *Id.* Plaintiffs submitted seven FOIA requests either to Immigration and Customs Enforcement ("ICE"), Customs and Border Patrol ("CBP"), or both, which are described in further detail below.

A. Requests for EID and IIDS Metadata and Database Schema

1. FOIA Request I

By letter dated October 13, 2010, Plaintiffs submitted a FOIA request to ICE for documentation related to the Enforcement Integrated Database ("EID"). *See* Defs.' Mot., Ex. 1, ECF No. 17-3 [hereinafter FOIA Request I]. The EID is a "shared common database repository for all records created, updated, and accessed by a number of [Department of Homeland Security ("DHS")] law enforcement and homeland security software applications." Defs.' Mot. for Summ. J., ECF No. 17 [hereinafter Defs.' Mot.], Decl. of Karolyn Miller, ECF No. 17-1 [hereinafter Miller Decl.], ¶ 12. EID "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], [CBP], and U.S. Citizenship and Immigration Services." *Id.* EID contains 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. *Id.* ICE uses the EID database to manage cases from the time of an undocumented immigrant's detention through the person's final case disposition. Defs.' Mot., Decl. of Fernando Pineiro, ECF No. 17-2 [hereinafter Pineiro Decl.], ¶ 47. Plaintiffs' first FOIA request sought:

> (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 . . . [and] (4) records that identify the [Database Management Software ("DBMS")] (e.g., Oracle, DB2, Sybase, SQL Server, etc.) including [the] Version No. used for the EID.

FOIA Request I at 1. In other words, Plaintiffs "sought a complete set of documentation on the [EID]." Pineiro Decl. ¶ 6 (internal quotation marks omitted).

2. *FOIA Request II*

On October 18, 2010, Plaintiffs submitted a second FOIA request to ICE for "a complete set of documentation on the 'ICE Integrated Decision Support . . . Database,'" known as "IIDS." Defs.' Mot., Ex. 8, ECF No. 17-3 [hereinafter FOIA Request II], at 1. IIDS is "a subset of the EID database repository . . . [that] provides a continuously updated snapshot of selected EID data." Miller Decl. ¶ 13. IIDS' "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." *Id.* "Specifically, IIDS contains biographic information, information about encounters between agents/officers and subjects, and apprehension and detention information about all persons in EID." *Id.* Plaintiffs' second FOIA request sought the same information regarding the IIDS database that the first request sought regarding the EID database. *See* FOIA Request II at 1.

In summary, FOIA Requests I and II sought documents that disclose the fields, variables, codes, and structures of the EID and IIDS databases. It appears that TRAC, as part of its goal to provide the public with information about law enforcement agencies, filed the requests in an attempt to learn what types of data ICE and CBP collect and rely upon to perform their immigration enforcement duties.

3. Government Response to FOIA Requests I and II

In response to FOIA Requests I and II, ICE conducted a search of the System Lifecycle Management repository database ("SLM"), which is "the authoritative place for technical documents associated with EID and IIDS." Defs.' Mot., Decl. of Jeff Wilson, ECF No. 17-6 [hereinafter Wilson Decl.], at 5. SLM documents are divided into sections and, after searching the EID and IIDS sections of the repository, ICE personnel reviewed responsive documents. *Id.* The agency then released 97 responsive pages, with redactions, and withheld the remaining responsive documents. Pineiro Decl. ¶ 19. CBP did not search its records in response to FOIA Requests I and II. *See* Pls.' Mot. at 10; Defs.' Opp'n to Pls.' Mot. for Summ. J. & Reply, ECF No. 25 [hereinafter Defs.' Opp'n & Reply], at 18.

B. Requests for Snapshots

1. FOIA Requests for Snapshots and Information About Snapshots

Plaintiffs also submitted FOIA requests to both ICE and CBP for "snapshots" of data from the EID database. As noted, the EID database includes "information related to the investigation, arrest, booking, detention, and removal of persons." Miller Decl. ¶ 12. ICE and CBP maintain several other databases, much like the IIDS database, that contain "subsets of EID data" and "provide . . . continuously updated snapshot[s] of selected EID data." Pls.' Mot., Decl. of Jehan A. Patterson, ECF No. 18-1 [hereinafter Patterson Decl.], Ex. A at 6. These snapshots allow CBP and ICE "to query EID data for operational or executive reporting purposes." *Id.* Collectively, the snapshots allow ICE to search all of the information contained within the EID database at a particular point in time. Wilson Decl. at 4. As described below, Plaintiffs' additional FOIA requests sought copies of certain snapshots.

On September 21, 2012, Plaintiffs submitted two FOIA requests to ICE. One sought information about snapshots. It requested "records identifying any extracts and 'snapshots' prepared from the [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 the extracts/snapshots, as well as the EID system time required in their preparation." Defs.' Mot., Ex. 16, ECF No. 17-3 [hereinafter FOIA Request III], at 1. The other request sought a copy of a snapshot itself, in particular, a "current 'snapshot' of ENFORCE prepared for [IIDS] system." Defs.' Mot., Ex. 19, ECF No. 17-3 [hereinafter FOIA Request IV], at 1. ENFORCE consists of several "applications" that allow "DHS personnel [to] create, modify, and access the data stored in the EID's central data repository." Patterson Decl., Ex. A at 2.

On February 25, 2013, Plaintiffs submitted a fifth FOIA request, this time to CBP, which sought a "current 'snapshot' of [the] EID database prepared for [the] CBP data warehouse." Defs.' Mot., Ex. 21, ECF No. 17-3 [hereinafter FOIA Request V], at 1. The next day, Plaintiffs submitted two final FOIA requests. The first was sent to ICE and sought "a current 'snapshot' of [the] EID database prepared for the EARM Data Mart." Defs.' Mot., Ex. 23, ECF No. 17-3 [hereinafter FOIA Requests VI], at 1. The second, which was sent to both ICE and CBP, sought "the current 'snapshot' of [the] EID database prepared for EID Data Mart." Defs.' Mot., Ex. 23, ECF No. 17-3 [hereinafter FOIA Requests VII], at 1. The EARM Datamart and the EID Datamart, like the

IIDS database, contain subsets of data from EID and are "typically used to generate management reports and statistics from EID data." Patterson Decl., Ex. A at 6. Specifically, the EARM Datamart, which is used to track cases of undocumented immigrants who are in the removal process, Pineiro Decl. ¶ 47, contains a host of information about immigration court proceedings and the detention statuses and locations of persons subject to such proceedings, Patterson Decl., Ex. A at 7. And the EID Datamart contains data on, among other things, arrests and removal processing, including personal information about persons subject to those proceedings. *Id.* at 7.

2. Government Response to FOIA Requests III through VII

In response to FOIA Request III, ICE disclosed nine pages of records that it asserted were responsive to the request, with redactions pursuant to FOIA exemptions 6, 7(C), and 7(E). Pineiro Decl. ¶ 27. Neither ICE nor CBP, however, produced copies of the snapshots Plaintiffs requested in FOIA Requests IV through VII.

3. Summary of FOIA Requests

In summary, TRAC submitted seven FOIA requests. Five were directed to ICE only, together requesting EID and IIDS metadata and database schema, as well as snapshots of data from the EID database and information about those snapshots. *See* FOIA Requests I, II, III, IV, and VI. One was directed to CBP only, requesting a snapshot of certain EID data. *See* FOIA Request V. And one was directed to both ICE and CBP, again seeking from each agency a snapshot of certain EID data. *See* FOIA Request VII.

C. Procedural History

Plaintiffs filed this action on January 29, 2014, alleging that Defendants' searches were inadequate and that Defendants improperly withheld responsive materials under FOIA. *See generally* Compl., ECF No. 1. On October 9, 2014, Defendants filed a Motion for Summary

Judgement. *See generally* Defs.' Mot. In it, Defendants argued that their search was adequate as they conducted searches in the SLM repository for documents responsive to Plaintiffs' request for the EID and IIDS metadata and database schema, and that they properly withheld responsive documents pursuant to Exemptions 3, 7(A), and 7(E). *Id.* at 10-11, 15-26. With regard to the snapshots, Defendants asserted that they were unable to produce any responsive documents, because "the snapshots Plaintiffs requested were not retained for the date ranges of the subject FOIA requests, . . . the requested information could not be produced with the technology currently in the Agency's possession, and . . . even if the information could be produced, Defendants were not capable of redacting the information." *Id.* at 11-12.

On November 13, 2014, Plaintiffs filed a Cross-Motion for Summary Judgment. *See generally* Pls.' Mot. In the Motion, Plaintiffs argued that Defendants' claimed FOIA exemptions are inapplicable. *Id.* at 14-26. They also disputed the assertion that Defendants are unable to produce the requested snapshots. *Id.* at 27-30. Plaintiffs further argued that Defendants' search was inadequate because Defendants: (1) did not sufficiently respond to FOIA Request III; (2) failed to search the EID and IIDS databases themselves for documents pertaining to the metadata and database schema of each system; and (3) failed to search CBP records. *Id.* at 31-32.

III. DISCUSSION

A. Standard of Review

Under Federal Rule of Civil Procedure 56, a court must grant summary judgment "if the movant 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). When a court is applying this standard, "the evidence of the non-movant is to be believed, and all justifiable inferences are to be drawn in his favor." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986). A dispute is "genuine" only if a reasonable fact-finder could find for the nonmoving party, while a fact is "material" only if it is capable of affecting the outcome of litigation. *Id.* at 248-49. A non-material factual dispute is insufficient to prevent the court from granting summary judgment. *Id.* at 249.

FOIA cases often are appropriately decided on motions for summary judgment. *See Defenders of Wildlife v. U.S. Border Patrol*, 623 F. Supp. 2d 83, 87 (D.D.C. 2009). A court may award summary judgment in a FOIA case using solely the information included in the agency's affidavits or declarations if they are "relatively detailed and non-conclusory," *SafeCard Servs., Inc. v. SEC*, 926 F.2d 1197, 1200 (D.C. Cir. 1991) (citations and internal quotation marks omitted), and describe "the documents and the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemption, and are not controverted by either contrary evidence in the record nor by evidence of agency bad faith," *Military Audit Project v. Casey,* 656 F.2d 724, 738 (D.C. Cir. 1981). "Unlike the review of other agency action that must be upheld if supported by substantial evidence and not arbitrary or capricious, the FOIA expressly places the burden 'on the agency to sustain its action' and directs the district courts to 'determine the matter *de novo*.'" *DOJ v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 755 (1989) (quoting 5 U.S.C. § 552(a)(4)(B)).

B. EID and IIDS Metadata and Database Schema

The court first considers Plaintiffs' challenge to Defendants' invocation of FOIA Exemptions 7(E), 7(A), and 3 to withhold and redact materials responsive to Plaintiffs' requests for EID and IIDS metadata and database schema. "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) (citation omitted). 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 *Dep't of State v. Ray*, 502 U.S. 164, 173 (1991)). But "an agency's justification for invoking a FOIA exemption is sufficient if it appears logical or plausible." *Larson v. Dep't of State*, 565 F.3d 857, 862 (D.C. Cir 2009) (citations and internal quotation marks omitted).

1. Exemption 7(E)

Defendants rely primarily on Exemption 7(E) to withhold records responsive to Plaintiffs' request for metadata and database schema. Once again, the metadata and database schema sought in this case are the fields, variables, codes, and structures of the EID and IIDS databases. Under Exemption 7(E), an agency may withhold information "compiled for law enforcement purposes" if, among other reasons, its release "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). Exemption 7(E) "sets a relatively low bar for the agency to justify withholding," *Blackwell v. FBI*, 646 F.3d 37, 42 (D.C. Cir. 2011), and "where an agency 'specializes in law enforcement, its decision to invoke [E]xemption 7 is entitled to deference,'" *Lardner v. DOJ*, 638 F. Supp. 2d 14, 31 (D.D.C. 2009) (quoting *Campbell v. DOJ*, 164 F.3d 20, 32 (D.C. Cir. 1998). This does not excuse an agency, however, from the requirement of describing its "justifications for withholding the information with specific detail." *ACLU v. Dep't of Defense*, 628 F.3d 612, 619 (D.C. Cir. 2011)).

Plaintiffs challenge Defendants' invocation of Exemption 7(E) on a host of grounds. Specifically, they argue that: (a) the records sought were not compiled for law enforcement purposes; (b) the records do not disclose law enforcement techniques, procedures, or guidelines; and (c) disclosure of the records does not present a risk of circumvention of the law. The court considers each of these arguments in turn.

a. Compiled for law enforcement purposes

Defendants contend that they "engage in law enforcement activity and the records responsive to the subject FOIA request were compiled for law enforcement purposes." Defs.' Mot. at 20. According to a declaration submitted by ICE's Deputy FOIA Officer, Fernando Pineiro, the databases at issue—namely, EID and IIDS—contain "law enforcement sensitive information relating to investigations, enforcement operations, and checks of other law enforcement databases." Defs.' Mot. at 20 (quoting Pineiro Decl. ¶ 47). ICE uses IIDS, in particular, "to rapidly run reports and queries on data stored in other ICE databases, particularly [EID]." Pineiro Decl. ¶ 47. Responding to Defendants' claim, Plaintiffs argue "[t]hat [just because] the databases themselves may contain information compiled for law enforcement purposes does not, as the government assumes, mean that all information *about* the databases—especially information that, like the information requested here, serves data management and administrative purposes—was also compiled for law enforcement purposes." Reply Mem. in Supp. of Pls.' Mot. for Summ. J., ECF No. 27 [hereinafter Pls.' Reply], at 2.

The court has little trouble rejecting Plaintiffs' argument. A record is deemed "compiled for a law enforcement purpose" so long as there is (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. *See Campbell*, 164 F.3d at 32; *see also Pratt v. Webster*, 673 F.2d 408, 420 (D.C. Cir. 1982). The latter requirement must be satisfied "to establish that the agency acted within its principal function of law enforcement, rather than merely engaging in a general monitoring of individuals' activities." *Pratt*, 673 F.3d at 420. Plaintiffs concede that Defendants use the EID and IIDS databases for law enforcement purposes—to assist ICE and CBP with deporting people who are unlawfully in the United States, to arrest those who violate federal immigration laws, and to track investigations and court proceedings of those apprehended. *See* Pls.' Mot. at 4. Thus, records concerning how these databases are constructed and how they operate—like the data itself—clearly have a rational "nexus" to Defendants' law enforcement duties. The second prong of the "law enforcement purpose" test is also satisfied because of the clear connection between the records and possible security risks or violations of law. These are not the kind of records compiled for generalized snooping of individuals' lives, but were prepared to effectuate the agencies' law enforcement responsibilities. The court thus concludes that the withheld records easily qualify as records or information "compiled for law enforcement purposes."

b. Techniques, procedures, or guidelines

Plaintiffs next argue that the withheld records concerning database metadata and database schema would not, if released, disclose "techniques," "procedures," or "guidelines" for law enforcement investigations or prosecutions, as those terms are used in Exemption 7(E). Plaintiffs contend that "the fact that data is used by law enforcement personnel in carrying out their duties does not mean that revealing information about a database discloses the techniques and methods that law enforcers employ in using it." Pls.' Reply at 4. For their part, Defendants offer the following, from ICE's Deputy FOIA Officer, Fernando Pineiro, in opposition to Plaintiffs' position:

> ICE employed certain law enforcement techniques and methods designed to obtain information in furtherance of the nation's immigration and customs laws, and ICE law enforcement officers use the database and systems that are the subjects of Plaintiffs' FOIA request to maintain that information and carry out those duties.

Pineiro Decl. ¶ 50; *see also* Defs.' Mot. at 20-22.

Although the court views the Pineiro Declaration as providing a rather thin explanation for why the metadata and database schema qualify as a law enforcement technique, procedure, or guideline, the court ultimately agrees with Defendants based on the Court of Appeals' decision in *Blackwell v. FBI*, 646 F.3d 37 (D.C. Cir. 2011), as well as analogous district court cases. In *Blackwell*, the FBI sought to protect under Exemption 7(E) "methods of data collection, organization and presentation contained" in certain reports. *Id.* at 42 (internal quotation marks omitted). The FBI's declarant explained that "the manner in which the data is searched, organized and reported to the FBI is an internal technique, not known to the public," and the "method was developed by [the vendor] to meet the specific investigative needs of the FBI." *Id.* (internal quotation marks omitted). Based on those averments (as well as an additional attestation concerning how disclosure could give rise to the potential risk of circumvention of the law), the Court of Appeals concluded that the FBI had properly invoked Exemption 7(E). *Id.*

Other cases from this Circuit are to similar effect. For instance, in *Strunk v. DOJ*, 905 F. Supp. 2d 142 (D.D.C. 2012), the court concluded that withheld computer screen transaction codes, computer transaction codes, and computer function codes—similar to the codes at issue here—from a CBP database known as TECS, though not themselves law enforcement "techniques and procedures," were protected "guidelines for law enforcement investigations and prosecutions" under Exemption 7(E). *Id.* at 148 (citation omitted). Similarly, in *Skinner v. DOJ*, 893 F. Supp. 2d 109 (D.D.C. 2012), the court agreed that computer access codes associated with the TECS database were, at the least, law enforcement guidelines under Exemption 7(E), *id.* at 114. And other decisions have treated law enforcement database codes or fields in the same way. *See Ortiz v. DOJ*, 67 F. Supp. 3d 109, 123 (D.D.C. 2014) (granting Exemption 7(E) protection to "violator identifier codes"); *Miller v. DOJ*, 872 F. Supp. 2d 12, 29 (D.D.C. 2012) (permitting agency to withhold law enforcement numerical database codes used to identify information and individuals, as well as codes "relate[d] to procedures concerning the use of law enforcement resources and databases . . ., as well as case program and access codes"); *McRae v. DOJ*, 869 F. Supp. 2d 151, 169 (D.D.C. 2012) (holding that "codes, case numbers, and other computer information pertaining to the TECS, NCIC, and databases maintained by the North Carolina authorities are techniques and procedures for law enforcement investigation").

Blackwell and these district court decisions teach that internal database codes, fields, and other types of identifiers used by law enforcement agencies to conduct, organize, and manage investigations and prosecutions qualify, at least, as law enforcement guidelines, if not also law enforcement methods and techniques. Thus, the court rejects Plaintiffs' argument that the EID and IIDS metadata and database schema do not qualify for withholding under Exemption 7(E).

c. Circumvention of the law

The parties' final area of disagreement about the application of Exemption 7(E) is also their most significant. They dispute whether disclosure of the metadata and database schema "could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 522(b)(7)(E). Defendants assert that disclosure of the EID and IIDS metadata and database schema would enable "individuals to access [ICE]'s law enforcement database, including its investigative files, manipulate data within those databases, and launch a full scale cyber-attack against [ICE]." Defs.' Mot. at 21. To establish the risk of such an attack, Defendants offer the affidavit of Karolyn Miller, an Information Technology Specialist in Information Security at ICE, who identifies a specific kind of risk—a Structured Query Language injection attack, or a "SQL injection attack," on the EID and IIDS databases. Miller Decl. ¶ 16. As Miller explains:

> 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. The program's error allows the attacker to then access otherwise restricted parts of the database to view or steal information . . . that will allow the attacker to not only access the full database, but . . . also potentially allow access to other parts of the IT system . . . by using the stolen credentials.

Id. She concludes that, "[s]hould ICE be required to provide . . . database schema, tables, codes, code values, and database version, ICE will have disclosed the exact information that an SQL [injection] attacker needs to penetrate the EID and IIDS databases and systems, and potentially the ICE network." *Id.* ¶ 19.

i. *<u>Plaintiffs' legal interpretation of Exemption 7(E)</u>*

Plaintiffs offer two rejoinders—one legal, the other factual—to Defendants' ominous prediction of a potentially debilitating cyber-attack resulting from disclosure. Plaintiffs first argue that, "[a]lthough a cyber-attack would undoubtedly constitute a violation of law, such a violation does not constitute circumvention of a relevant law within the meaning of Exemption 7(E)." Pls.' Mot. at 16. Instead, according to Plaintiffs, "the exemption allows an agency to withhold techniques, procedures, and guidelines that it uses to enforce particular laws . . . if disclosure of those techniques, procedures, or guidelines would allow an individual to circumvent *those* laws." *Id.* In other words, Plaintiffs contend that Exemption 7(E) applies only if the risk that there will be a violation of law relates to those laws that the subject law enforcement agency is tasked with enforcing. Plaintiffs thus argue that an unlawful cyber-attack cannot serve as a basis for withholding EID and IIDS metadata and database schema because such information, if disclosed, does not risk circumvention of the laws enforced by Defendants.

The FOIA statute, however, cannot be read so narrowly. Exemption 7(E) plainly states that withholding is permissible under that provision if "disclosure could reasonably be expected to risk circumvention *of the law*"—"the law," period. 5 U.S.C. § 552(b)(7)(E). Congress did not qualify or modify "the law" in any way to circumscribe the types of laws that might be violated in the event of disclosure for Exemption 7(E) to apply. Thus, a plain reading of the statute does not support Plaintiffs' interpretation.

Nor have courts read the exemption as Plaintiffs have proposed. Indeed, courts in this District have recognized the risk of a cyber-attack or a breach of a law enforcement database as valid grounds for withholding under Exemption 7(E). In *Skinner*, the court upheld the agency's decision to withhold data under Exemption 7(E) where the agency showed that release of the subject data would "(1) permit unauthorized users to avoid recognition, instant detection and apprehension, (2) give them near-unfettered access to one of the nation's most critical electronic law enforcement infrastructures, and (3) arm these intruders with the ability to irreparably corrupt the integrity of [the database] by altering or manipulating it." 893 F. Supp. 2d at 113 (internal quotation marks omitted). Likewise, in *Strunk*, the court recognized a risk of circumvention where disclosure of data could "facilitate[ ] access to and navigation through [a law enforcement database] and reveal[ ] mechanisms for access to and navigation through [the database]." 905 F. Supp. 2d at 147. There, the agencies asserted that "individuals who knew the meaning of the codes . . . would gain access to CBP law enforcement techniques and procedures that would permit them to . . . corrupt[ ] the integrity of ongoing investigations." *Id.* at 148. *Skinner* and *Strunk* make clear that the potential for a cyber-attack or data breach is the kind of risk of circumvention of the law that justifies withholding under Exemption 7.

ii. *Plaintiffs' factual challenge to the asserted risk of a cyber-attack*

This case, however, differs from *Skinner* and *Strunk* in one important respect: Plaintiffs here have aggressively challenged Defendants' assertion that disclosure of the metadata and database schema would expose the EID and IIDS databases to a SQL injection attack. In support, Plaintiffs have offered the declaration of an expert in data security, Dr. Paul Clark, President and Chief Technology Officer of SecureMethods, Inc., and Paul C. Clark, LLC,[1] who disputes the potential for a SQL attack. He explains:

> A SQL injection attack is a type of remote execution attack. In other words, someone who is not physically on the premises where a computer system is located nonetheless can launch an attack by transmitting malicious instructions through a web interface that has a direct connection to a database that will accept and execute such instructions . . . . [R]emote execution is *not a credible threat* to the EID or IIDS systems . . . [because] there is no publicly accessible web interface to the EID or IIDS, nor do agencies outside of [DHS] have access to the database systems.

Pls.' Mot., Decl. of Paul C. Clark, ECF No. 18-3 [hereinafter Clark Decl.], ¶¶ 11-12 (emphasis added).

Defendants offer a relatively limp response to Dr. Clark's critique. They do not disagree that a hacker would require an external access point to execute a SQL injection attack; nor do they claim that the EID or IIDS databases are in fact accessible through an external access point. Rather, through the affidavit of Jeff Wilson, Unit Chief of the Information Technology Management Unit within Enforcement and Removal Operations, Law Enforcement and Systems Analysis at ICE, Defendants state: "[T]here are still dangers associated with providing information and records associated with system development, data tables and fields, outage times, etc., whether or not the database has a 'publically accessible web interface.'" Defs.' Opp'n & Reply, Suppl.

[1] *See* Pls.' Mot., Decl. of Paul C. Clark, ECF No. 18-3, at 11.

Decl. of Jeff Wilson, ECF No. 25-1 [hereinafter Wilson Suppl. Decl.], ¶ 9. Wilson cites as the sole example a 2014 cyber-attack against Home Depot, which was executed using malware inserted at point-of-sale machines in stores in the United States and Canada. *Id.* Wilson Suppl. Decl. ¶ 9. Wilson adds:

> Intimate knowledge of tables, codes, and schemas can be used to create a more sophisticated attack that lasts days, weeks or even months. Additional technical dangers include: cross site scripting, session hijacking, SQL injection, race conditions, unformatted error messages, improper html rendering and submittals, among others.

Id. ¶ 10. But nowhere does he say that any of those "additional technical dangers" could be accomplished when a system, like the one at issue here, has no an external access point.

Plaintiffs offer an obvious retort to Wilson's statements. In a supplemental declaration, Dr. Clark states: "In the Home Depot example [Wilson] cites, access was obtained not through a web interface, but through point-of-sale devices that connected to Home Depot's system. ICE obviously does not use point-of-sale devices that would provide an attacker with access to its systems, and Mr. Wilson does not suggest that any comparable means of access to ICE's systems exists." Pls.' Reply, Suppl. Decl. of Paul C. Clark., ECF 27-2 [hereinafter Clark Suppl. Decl.], ¶ 4. When pressed at oral argument, counsel for Defendants was unable to identify any SQL injection attacks that have occurred without a public access point and asked to further brief the question whether a SQL injection attack could be achieved only via a public access point. Hr'g Tr. at 21:3-23:14, Oct. 28, 2015 (Draft).

In evaluating whether Plaintiffs have carried their burden of showing a risk of circumvention of the law, the court is fully cognizant of the low bar that the Court of Appeals has set for establishing such risk. *See, e.g.*, *Pub. Employees for Envtl. Responsibility v. U.S. Section,* *Int'l Boundary & Water Comm'n*, *U.S.-Mexico*, 740 F.3d 195, 204-05 (D.C. Cir. 2014); *Blackwell v. FBI*, 646 F.3d at 42. Trial courts are to:

> [L]ook[ ] 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.

Mayer Brown LLP v. IRS, 562 F.3d 1190, 1193 (D.C. Cir. 2009). Courts must heed that low bar, especially in cases where an agency has warned that disclosure could lead to a cyber-attack on, or security breach of, an agency data system containing sensitive law enforcement and personal information. Judges are not cyber specialists, and it would be the height of judicial irresponsibility for a court to blithely disregard such a claimed risk.

But the standard of review of a claimed 7(E) exemption, while highly deferential, is not "vacuous." *Campbell*, 164 F.3d at 32 (quoting *Pratt*, 673 F.2d at 421). Courts have a responsibility to ensure that an agency is not simply manufacturing an artificial risk and that the agency's proffered risk assessment is rooted in facts. Based on the present record, the court cannot find that Defendants have carried their burden of showing that disclosure of the IED and IIDS metadata and database schema increases the risk of a cyber-attack of the kind Defendants posit. The sole risk that Defendants claim might be heightened by the release of metadata and database schema is that of a SQL injection attack. On the present record, however, it is undisputed that a SQL injection attack requires an external point of entry, such as a website or point-of-sale machine, and that the IED and IIDS databases are not so exposed. The court is thus left unconvinced, at this juncture, that the sole risk of circumvention of the law claimed by Defendants—a SQL injection attack—would be increased if the requested metadata and database schema were disclosed. The court, therefore, denies Defendants' Motion for Summary Judgment as to its invocation of

Exemption 7(E) to withhold information concerning IED and IIDS metadata and database schema.[2]

The court, however, will not at this juncture order Defendants to disclose the withheld material. Rather, in the exercise of its discretion, the court will permit Defendants to supplement the record with additional affidavits or other evidence to establish that disclosure of the IED and IIDS metadata and database schema will increase the risk of a cyber-attack, data breach, or any other circumvention of the law.[3] *See Wolf v. CIA*, 569 F. Supp. 2d 1, 10 (D.D.C. 2008) ("Where an agency's declarations are deficient, courts generally will request that an agency supplement its supporting declarations rather than order discovery." (citation and internal quotation marks omitted)); *see also Hall v. CIA*, 668 F. Supp. 2d 172, 188-93 (D.D.C. 2009) (granting in part and denying in part the agency's and the plaintiff's cross-motions for summary judgment, and permitting the agency to submit a "supplemental filing" in support of its invocation of certain FOIA exemptions).

2. *Exemption 3*

Defendants alternatively argue that their withholding of metadata and database schema is justified under FOIA Exemption 3. Generally speaking, that exemption protects a record from disclosure if it has been "specifically exempted from disclosure by statute." 5 U.S.C. § 552(b)(3). Here, Defendants have argued that the withheld materials are exempt from disclosure under the

[2] Defendants also invoke Exemption 7(A) to justify withholding the metadata and database schema. However, Defendants' invocation of Exemption 7(A) relies on arguments substantially identical to those presented in connection with their Exemption 7(E) claim. That is, disclosure of the requested information would expose the databases to potential cyber-attacks. *See* Defs.' Opp'n and Reply at 22-23; Hr'g Tr. 26:5-28:9. Thus, for the same reason that the court has denied summary judgment on Defendants' invocation of Exemption 7(E), it does so as to Defendants' invocation of Exemption 7(A).

[3] Defendants' briefing also suggests the possibility of an "inside job" where someone within ICE or CBP, who otherwise does not have access to the requested information, could use it to gain unauthorized access to the databases. *See* Defs.' Opp'n. and Reply at 10; *see also* Hr'g Tr. at 24:8-25:3. But Defendants have not presented any evidence of how the requested disclosures might increase the risk of such an attack. Defendants may wish to address this risk in its supplemental submission.

Federal Information Security Management Act ("Management Act"), 44 U.S.C. §§ 3541-49. They are incorrect.

Exemption 3 applies only if a statute "requires that matters be withheld from the public in such a manner as to leave no discretion on the issue" or "establishes particular criteria for withholding or refers to particular types of matters to be withheld." 5 U.S.C. § 552(b)(3)(A). Exemption 3 further provides that, "if [the statute was] enacted after the date of enactment of the OPEN FOIA Act of 2009," Exemption 3 applies only if the statute "specifically cites to this paragraph." *Id.* § 552(b)(3)(B).

The statute upon which Defendants rely—the Management Act—was repealed in its entirety on December 18, 2014—after this case was filed—and replaced by the Federal Information Security Modernization Act of 2014 ("Modernization Act"), 44 U.S.C. § 3551 *et seq.* (2014). As the Modernization Act is the law in effect at the time the court is rendering its decision, it is the controlling law in the present dispute. *See Bradley v. School Bd. of City of Richmond*, 416 U.S. 696, 711 (1974) (stating the "principle that a court is to apply the law in effect at the time it renders its decision, unless doing so would result in manifest injustice or there is statutory direction or legislative history to the contrary").

The Modernization Act does not enable Defendants to invoke Exemption 3 here for two reasons. First, because the Modernization Act was enacted after the OPEN FOIA Act of 2009, for it to protect records from disclosure under Exemption 3 it must "specifically cite[ ] to [Exemption 3]." 5 U.S.C. § 552(b)(3)(B). It does not do so. Second, to the extent that the Modernization Act does cite to FOIA, it does not alter agencies' obligations under the FOIA statute. The Modernization Act expressly states that "[n]othing in this subchapter . . . may be construed as affecting the authority of . . . the head of any agency, with respect to the authorized use or disclosure of information, including . . . the disclosure of information under section 552 of title 5." 44 U.S.C. § 3558. Therefore, Defendants' claim that the requested materials can be withheld pursuant to Exemption 3 fails.

C. Copies of Snapshots of Data from the EID Database

The parties' second major dispute concerns Defendants' non-production of copies of "snapshots" of data from the EID database. Again, "snapshots" are continuously updated extracts of portions of the EID database that enable Defendants to search and manipulate the EID data. Plaintiffs assert that Defendants have not complied with FOIA because they failed to disclose copies of the requested snapshots and did not perform an adequate search for them. Defendants offer two reasons why they cannot comply with Plaintiffs' requests for copies of snapshots. First, they argue that their "document system is not capable of producing the information for distribution to Plaintiffs." Defs.' Mot. at 13. Second, they argue that even if they could produce the snapshots, "Defendants lack[ ] the technology to redact the information." *Id.* at 14.

Under FOIA, "an agency shall provide the record in any form or format requested by the person if the record is *readily reproducible* by the agency in that form or format." 5 U.S.C. § 552(a)(3)(B) (emphasis added). The key term, "readily reproducible," "is not . . . synonymous with technical[ly] feasible." *Scudder v. CIA*, 25 F. Supp. 3d 19, 38 (D.D.C. 2014). Rather, "[t]he Court may consider the burden on the defendant agency in determining whether the documents at issue are 'readily reproducible.'" *Id.* To justify withholding otherwise responsive materials, the "agency's evidence of burden . . . must be not only compelling, but also demonstrate that compliance with a request would impose a *significant* burden or interference with the agency's operation." *Public.Resource.Org v. IRS*, 78 F. Supp. 3d 1262, 1266 (N.D. Cal. 2015) (citing *TPS, Inc. v. DOD*, 330 F.3d 1191, 1195 (9th Cir. 2003)). Among the factors that a court may consider in assessing the claimed burden are the amount of time, expense, and personnel that would be required to complete document searches and production, as well as whether the agency has the existing technology or would have to purchase new technology to perform those tasks. *See Wolf v. CIA*, 569 F. Supp. 2d at 9 ("Courts often look for a detailed explanation by the agency regarding the time and expense of a proposed search in order to assess its reasonableness." (citation omitted)); *Pinson v. DOJ*, 80 F. Supp. 3d 211, 217 (D.D.C. 2015) (holding that DOJ did not carry its burden by merely asserting that the search would require a "burdensome effort" without offering estimates of "the time required to conduct [the] requested search, the cost of such a search, or the number of files that would have to be manually searched").

Consistent with these principles, courts have held that agencies need not disclose records when conducting a search for requested materials would impose an unreasonable burden. *See, e.g.*, *Nation Magazine, Washington Bureau v. U.S. Customs Serv.*, 71 F.3d 885, 891-92 (D.C. Cir. 1995) (determining that a request that required an agency to search through 23 years of unindexed files imposed an unreasonable burden); *Am. Fed'n of Gov't Employees, Local 2782 v. U.S. Dep't of Commerce*, 907 F.2d 203, 208-09 (D.C. Cir. 1990) (holding that a request that required a search of "every chronological office file and correspondent file, internal and external, for every branch office [and] staff office" was overbroad); *Nat'l Sec. Counselors v. CIA.*, 960 F. Supp. 2d 101, 161-62 (D.D.C. 2013) (concluding that a request that sought copies of all federal intelligence agency records pertaining to a supercomputer and required a search of all agency offices was so broad as to impose an unreasonable burden upon the agency). Courts also have held that agencies are excused from complying with FOIA requests where "review[ing], redact[ing], and arrang[ing] for inspection [of] a vast quantity of material" presents an unreasonable burden. *Am. Fed'n of Gov't Employees*, 907 F.2d at 209; *see also Vietnam Veterans of Am. Conn. Greater Hartford Chapter*

120 v. DHS, 8 F. Supp. 3d 188, 203 (D. Conn. 2014) (FOIA request for which agency would need to locate, review, and make heavy redactions to 26,000 packets, each of which contained 50 pages, was unreasonably burdensome); *Hainey v. Dep't of Interior*, 925 F. Supp. 2d 34, 45 (D.D.C. 2013) (holding that it would be unreasonably burdensome to require the agency to search and review every email sent or received by 25 different employees throughout a two-year time period). Particularly relevant here, one court has held that the process of making redactions to 20 million responsive records within a database was sufficiently burdensome to justify the agency's withholding of the entirety of the requested information. *See Ayuda, Inc. v. FTC*, 70 F. Supp. 3d 247, 276-77 (D.D.C. 2014) ("[B]ecause the agency aims to protect the private information of citizens by withholding the data fields at issue, and because the manual review needed for redacting such information is unreasonably burdensome, the Court concludes that the FTC properly withheld the data fields.").

Consistent with the above cases, the court finds that Defendants have demonstrated that producing and redacting the requested snapshots would be unduly burdensome. According to Defendants' affiant Jeff Wilson, "[c]urrently, there is no specific product, report or snapshot generated during the Extract-Transform-Load (ETL) process where information from the EID is transferred to IIDS and the datamarts . . . . [T]his process is automatic and occurs through a link established between two databases with no tangible extract files." Wilson Suppl. Decl. ¶ 15; *see also* Wilson Decl. at 8 ("To produce an extract in a format that could be consumed by the external entity, a new record would need to be created. It would require the design, development, and implementation of a different process for this new record that does not include law enforcement sensitive and/or personally identifiable information[.]"). In other words, according to Wilson, when EID data is collected, organized, and transferred to a functional database like IIDS, no reproducible extract or copy of the transferred data, or snapshot, is created to provide to a FOIA requester. Wilson adds: "ICE does not currently have the technology to [produce the requested snapshots]. It is difficult to assess what it would take to provide a severable copy because the EID is comprised of so many data elements." Wilson Decl. at 9. At a minimum, Wilson explains, duplication and production of snapshots would "require a new contract to facilitate the extract process and associated databases in the hundreds of thousands to millions of dollars." *Id.* The contract would have to provide for the hiring of additional information technology specialists, including experts in database design and maintenance, large data storage and transfer, networking, and programming, as well as the hiring of experts to remove or redact sensitive law enforcement data. *Id.*

And, according to Wilson, even if Defendants could replicate the snapshot for production, they would face tremendous challenges in redacting sensitive personal and law enforcement material, which even Plaintiffs concede are subject to valid FOIA exemptions. The tables available in the EID consist of more than *6.7 billion* rows of data, with the total amount of information contained within the EID exceeding five terabytes. *Id.* at 7. Wilson equated the volume of data to "1.8 million songs on an iPod" or an audiobook that "would take approximately 9.5 years to read." *Id.* Further employing the example of an iPod, Wilson stated that redacting exempt information would be akin to "redacting every artist, album, and song name as well as significant portions of the song[s]." *Id.* at 8. According to Wilson, "[a]t this particular time, the ICE FOIA Office does not have the existing technology or expertise for processing this data." Wilson Suppl. Decl. ¶ 16. Although Wilson could have been more descriptive in explaining precisely what it would take to redact exempt information and why such process would be unduly burdensome, he does state the following: "The redaction process for this request is expensive for a federal agency. It requires a modification to an existing contract, clearances, background screenings, training, and ramp up time." *Id.*

Plaintiffs dispute Defendants' contention that producing and redacting the requested snapshots would impose an undue burden on the agencies. Plaintiffs offer their own expert declaration from Michael Hasan, a software engineer employed by Plaintiffs' research institute, TRAC. To rebut Defendants' contention that reproducing a snapshot would impose an undue burden, Hasan states that "[e]xtraction is a built-in functionality of any commercial [DBMS] software that allows any database object or table to be queried and extracted into text or another electronic representation. . . . Thus, it should be an easy and inexpensive process to extract data using such software." Pls.' Mot., Decl. of Michael Hasan, ECF No. 18-4 [hereinafter Hasan Decl.], ¶ 10. As to Defendants' contentions concerning the burdensomeness of redacting the snapshots, Hasan states, "[r]edaction is another built-in functionality that is common across commercial DBMS packages. It is a trivial matter to redact a column of information (for example, a column containing Social Security numbers of individuals apprehended by defendants) by executing a simple . . . command that either deletes the data in the column or replaces the data with a special symbol to denote redaction." *Id.* ¶ 13.

Although Hasan's Declaration raises some questions about whether the snapshots are indeed readily reproducible and redactable, the court ultimately finds those questions insufficient to create a genuine dispute of material fact that would preclude a grant of summary judgment in Defendants' favor. FOIA requires courts to "accord *substantial weight* to an affidavit of an agency concerning the agency's determination as to technical feasibility . . . and reproducibility[.]" *See* 5 U.S.C. § 552(a)(4)(B) (emphasis added); *see also Scudder*, 25 F. Supp. 3d at 39 ("[S]ubstantial deference is due an agency's 'reproducibility' determination[.]"). Here, Defendants' declarant, Jeff Wilson, has attested, based on his specific knowledge of and experience with the EID database and associated datamarts that replicating and redacting the snapshots would create an undue burden on the agencies. The court, as it must, accords that view substantial weight. Plaintiffs' declarant, though an expert in the field of database systems and management, has not offered any evidence that specifically rebuts Wilson's assertions about the agencies' present technological capabilities *as to the EID database and associated datamarts* or regarding the burden that reproduction and redaction of the snapshots would impose on them. Instead, Hasan offers only observations about commercial databases in general—his declaration reveals no specific knowledge about the EID database and its associated operations. Hasan, naturally, is limited by his lack of first-hand experience with the EID database and the datamarts at issue in this case. But once, as here, an agency has proffered a declaration as to the technical feasibility and reproducibility of a records request—which, by statute, must be accorded substantial weight—a plaintiff must offer more than generalities about technical capabilities of generic systems to overcome or raise questions about that declaration. Plaintiffs have failed to do so here.

Plaintiffs make one additional argument in an effort to rebut Defendants' contention that reproducing and redacting would impose an undue burden. Plaintiffs argue that Defendants must be able to produce and redact the snapshot because they have previously provided Plaintiffs with redacted portions of snapshots in response to other FOIA requests. Long Decl. ¶¶ 16-20. Defendants do not deny the past productions but argue that Plaintiffs' present requests are meaningfully different in scope and scale. Whereas Plaintiffs' previous, fulfilled requests sought specific information contained in the snapshots, the present requests seek the snapshots in their entirety. Defs.' Mot. at 14. For example, one previous request sought "anonymous case-by-case information on each removal and return *for January 2014*." Wilson Suppl. Decl. ¶ 12 (emphasis added). "The request specifically asked for 54 data elements for each individual removed/returned; the data elements include[d], inter alia, biographical information, criminal history, and immigration history for every individual removed/returned for a limited time period." *Id.* As to that request, ICE reviewed the relevant information and created *new spreadsheets* in order to provide it to Plaintiffs. *See id.* ICE also created codes that it used to alter exempt information contained in the requested data set so that such information was not released. *See* Hr'g Tr. at 15:1-16; *see also* Wilson Suppl. Decl. ¶ 12. Defendants thus contend that these past productions serve as poor comparators for the present, far more expansive requests.

The court agrees. The court again accords substantial weight to the representations of Defendants' affiant, Jeff Wilson. According to Wilson, a request for a snapshot of the entire database is "vastly different" from Plaintiffs' previous requests and, as a consequence, the manner in which ICE responded to the prior requests is "wholly inadequate for responding to a request for all the data replicated at unspecified points in time into other datamarts." Wilson Suppl. Decl. ¶ 13. Wilson adds that "the replication or copying of all data from EID data into the IIDS, and other datamarts[,] is not a pull of data," which was sufficient to respond to past requests. *Id.* Plaintiffs have not offered any evidence specific to the databases at issue here that rebuts those contentions. The court therefore concludes that FOIA does not require Defendants to produce redacted copies of the requested snapshots.

D. Request for Discovery

In a related argument, Plaintiffs request that the court allow them to conduct discovery on the factual issues concerning Defendants' capacity to produce and redact the extracts and snapshots from their databases. They argue that they "have introduced facts casting serious doubt on defendants' assertions that they lack the technology to produce and redact data extract files and that they would have to spend 'hundreds of thousands to millions of dollars,' Wilson Decl. at 9, on a contract to create a new database." Pls.' Mot. at 30.

Courts have "broad discretion to manage the scope of discovery" in FOIA cases. *SafeCard Servs.*, 926 F.2d at 1200. "Discovery in FOIA is rare and should be denied where an agency's declarations are reasonably detailed, submitted in good faith and the court is satisfied that no factual dispute remains." *Schrecker v. DOJ*, 217 F. Supp. 2d 29, 35 (D.D.C. 2002); *see also Baker & Hostetler LLP v. U.S. Dep't of Commerce*, 473 F.3d 312, 318 (D.C. Cir. 2006). Here, Defendants have set forth detailed affidavits explaining that they currently lack the technology to produce and redact copies of the requested snapshots and that acquiring the necessary technology and marshalling the resources necessary to produce and redact copies of the snapshots would be unduly burdensome. Although Plaintiffs have offered rebuttal declarations that raise some questions about Defendants' assertions, for the reasons already discussed, Plaintiffs have not offered any evidence that is specific to the EID and other databases at issue in this case, to create a factual dispute that might otherwise justify allowing Plaintiffs to take discovery. *Cf. Scudder*, 25 F. Supp. 3d at 37 (finding that factual disputes existed where the plaintiff "provided reasonable evidence, based on his purported personal experience and observations, that the documents requested *do* exist in the format requested . . . even alert[ing] the defendant's FOIA staff as to where within the defendant's computer systems the electronically stored documents [we]re located"). Accordingly, Plaintiffs' request for discovery is denied.

E. Adequacy of the Search

Plaintiffs argue that Defendants' search was inadequate in three ways. First, Plaintiffs argue that Defendants failed to provide any information regarding their search for FOIA Request

III—that is, "records identifying any extracts and 'snapshots' prepared from the [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 the extracts/snapshots, as well as the EID system time required in their preparation." FOIA Request III at 1; *see also* Pls.' Mot. at 31. Second, they argue that Defendants' search for the metadata and database schema was inadequate because Defendants did not search the EID and IIDS databases for responsive records. Pls.' Mot. at 31-32. Finally, Plaintiffs argue that Defendants' search was inadequate because they failed to search any CBP records. *Id.* at 32.

FOIA requires an agency to conduct a search for responsive records that is "reasonably calculated to discover the requested documents." *SafeCard Servs.*, 926 F.2d at 1201. "In general, the adequacy of a search is 'determined not by the fruits of the search, but by the appropriateness of [its] methods.'" *Hodge v. FBI*, 703 F.3d 575, 579 (D.C. Cir. 2013) (quoting *Iturralde v. Comptroller of the Currency*, 315 F.3d 311, 315 (D.C. Cir. 2003)). In order to prevail on summary judgment, "the agency must show that it made a good faith effort to conduct a search for the requested records, using methods which can be reasonably expected to produce the information requested." *Oglesby v. U.S. Dep't of the Army*, 920 F.2d 57, 68 (D.C. Cir. 1990) (citation omitted). To carry this burden, the agency may submit a "reasonably detailed affidavit, setting forth the search terms and the type of search performed, and averring that all files likely to contain responsive materials (if such records exist) were searched." *Id.* "The adequacy of the search, in turn, is judged by a standard of reasonableness and depends, not surprisingly, upon the facts of each case." *Weisberg v. DOJ*, 745 F.2d 1476, 1485 (D.C. Cir. 1984) (citation omitted).

The court agrees with Plaintiffs' first contention that Defendants have not explained what search, if any, they undertook to locate extract identification and preparation records sought in

FOIA Request III. Indeed, the government does not even respond to this argument. *See* Defs.' Reply at 17-18. Because Defendants do not address what search, if any, they conducted, the court will deny summary judgement as to the adequacy of their search in response to FOIA Request III. *See Oglesby*, 920 F.2d at 68. Defendants shall submit an affidavit that sets forth the search efforts undertaken in response to FOIA Request III.

Plaintiffs next argue that the search Defendants conducted in response to FOIA Requests I and II was inadequate. Plaintiffs' first two FOIA requests sought metadata and data schema from the EID and IIDS databases, including "records identifying the database tables . . . records defining the codes . . . database schema, and records that identify the DBMS software." FOIA Request I at 1; FOIA Request II at 1. According to declarant Jeff Wilson, ICE conducted the following search:

> On July 15, 2014, the ICE [Office of the Chief Information Officer ("OCIO")] searched the [SLM] repository and located 2,793 documents. The SLM repository is the authoritative place for technical documents associated with the EID and IIDS. As a result, no other databases were required to be searched by OCIO. SLM documents are organized by sections so personnel located the "EID" and "IIDS" sections throughout the repository and transferred applicable documents for review.

Wilson Decl. at 5. Plaintiffs contend that this search was inadequate because Defendants did not search the EID and IIDS databases themselves for responsive documents. Pls.' Mot. at 31-32. According to Plaintiffs, "[l]ocating and copying the responsive information from the [EID and IIDS] databases would require only the execution of simple commands, and would provide the most accurate and current records responsive to the requests for database schema and code tables." Pls.' Reply at 24 (citing Pls.' Reply, Second Decl. of Michael Hasan, ECF No. 27-3 [hereinafter Sec. Hasan Decl.], ¶¶ 9-10).

The court disagrees with Plaintiffs and finds that Defendants' search of the SLM repository for the requested records was adequate. "There is no requirement that an agency search every record system." *Oglesby*, 920 F.2d at 68 (citations omitted). The agency responded to the FOIA request by searching the "authoritative" database where responsive records were likely to be held. It identified the sections of that database where responsive documents were likely to be found and reviewed the responsive documents. Though Plaintiffs may be correct that "[t]he database schema and [metadata] are actually a built-in part of any modern database," Sec. Hasan Decl. ¶ 10, and therefore, are necessarily contained within the EID and IIDS databases, they have not offered any reason to believe that responsive records—other than the database schema and codes themselves, which Defendants are not required to produce at this juncture—would be found within the databases. Absent such a showing, the court is satisfied that Defendants conducted a proper search for the EID and IIDS database schema and metadata. *See Mobley v. CIA*, Civ. No. 11-cv-02072, Civ. No. 11-cv-02073, 2015 WL 7423687, *8 (D.C. Cir. Nov. 13, 2015) ("Agency affidavits—so long as they are 'relatively detailed and non-conclusory'—are 'accorded a presumption of good faith, which cannot be rebutted by 'purely speculative claims about the existence and discoverability of other documents.'" (citations omitted)).

Plaintiffs last contend that the search was inadequate because Defendants failed to search CBP records for responsive documents. Of Plaintiffs' seven FOIA requests at issue in this case, only FOIA Requests V and VII were directed to CBP. Both of those were requests for copies of the requested snapshots. Because the court already has concluded that Defendants need not produce copies of snapshots, the court does not reach the issue of the adequacy of Defendants' search of CBP records.

IV. CONCLUSION AND ORDER

For the reasons set forth above, Defendants' Motion is granted in part and denied in part and Plaintiffs' Cross-Motion is granted in part and denied in part. Judgment is entered in favor of

Defendants as to (1) the adequacy of the search for FOIA Requests I and II and (2) their withholding of copies of snapshots in response to FOIA Requests IV through VII.

As for the grounds on which the court has denied Defendants' Motion, within 30 days of this date, Defendants shall be permitted to supplement their summary judgment briefing with additional evidence that supports their assertions that (1) disclosure of metadata and database schema "could reasonably be expected to risk circumvention of the law" under Exemption 7(E) and (2) they have conducted an adequate search for records in response to FOIA Request III. Thereafter, within seven days, Plaintiffs shall notify the court if they intend to challenge the newly submitted evidence, and if so, the parties shall propose a briefing schedule.

Amit Mehta

Dated: December 14, 2015

Amit P. Mehta
United States District Judge