UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

SUSAN B. LONG and DAVID BURNHAM, Plaintiffs, v. IMMIGRATION AND CUSTOMS ENFORCEMENT and CUSTOMS AND BORDER PROTECTION, Defendants.	Civil Action No. 1:14-cv-0109 Judge John D. Bates

PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT

Pursuant to Federal Rule of Civil Procedure 56, plaintiffs Susan B. Long and David Burnham hereby move for summary judgment in this case brought under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, on the ground that there is no genuine issue of disputed material fact and that plaintiffs are entitled to judgment as a matter of law. Defendants Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP) have not demonstrated that the withheld records are exempt from disclosure under 5 U.S.C. § 552(b)(7)(E) or demonstrated that there is any other basis for withholding them under FOIA. Accordingly, judgment should be entered for plaintiffs.

In support of this motion and in opposition to defendants' motion for summary judgment, plaintiffs submit the accompanying Memorandum of Points and Authorities in Support of Plaintiffs' Motion for Summary Judgment and in Opposition to Defendant's Motion for Summary Judgment, Plaintiffs' Statement of Material Facts as to Which There Is No Genuine

Issue, the Declaration of Jehan A. Patterson and exhibits annexed thereto, the Declaration of Susan B. Long and exhibits annexed thereto, the Declaration of Paul C. Clark and exhibit annexed thereto, the Declaration of Michael Hasan and exhibit annexed thereto, and a proposed order. Plaintiffs also rely on those portions of defendants' declarations cited herein.

Respectfully submitted,

s/ Jehan A. Patterson
Jehan A. Patterson
DC Bar No. 1012119
Scott L. Nelson
DC Bar No. 413548
PUBLIC CITIZEN LITIGATION GROUP
1600 20th Street NW
Washington, DC 20009
Tel: (202) 588-1000

Dated: November 13, 2014

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

SUSAN B. LONG and DAVID BURNHAM, Plaintiffs, v. IMMIGRATION AND CUSTOMS ENFORCEMENT and CUSTOMS AND BORDER PROTECTION, Defendants.	Civil Action No. 1:14-cv-0109 Judge John D. Bates

MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT AND IN OPPOSITION TO DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

Jehan A. Patterson
DC Bar No. 1012119
Scott L. Nelson
DC Bar No. 413548
PUBLIC CITIZEN LITIGATION GROUP
1600 20th Street NW
Washington, DC 20009
(202) 588-1000

November 13, 2014

Counsel for Plaintiffs

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES, REGULATIONS AND RULES

MISCELLANEOUS

INTRODUCTION

In this Freedom of Information Act (FOIA) case, Transactional Records Access Clearinghouse (TRAC) co-directors Susan B. Long and David Burnham seek records relating to immigration enforcement databases owned and operated by Immigrations and Customs Enforcement (ICE) and Customs and Border Protection (CBP). Specifically, Long and Burnham seek records identifying the names of database tables and fields, records defining the database codes used to record data, records setting forth the database schema (that is, the way the various database tables connect to each other), and records identifying the software used to construct ICE's Enforcement Integrated Database (EID) and ICE's Integrated Decision Support (IIDS) database. They also seek records identifying various extracts of data from the EID and records concerning the preparation, senders, and recipients of those extracts. Finally, Long and Burnham have requested snapshots of data that are extracted from the EID and transferred to several associated databases on a regular basis.

Information contained in the EID and associated databases constitutes the official records of the government concerning its enforcement of federal criminal and immigration laws. The requested records will allow TRAC to analyze the defendants' decisions concerning, among other things, whether their actual actions and activities are achieving defendants' stated goals when executing their immigration and law enforcement responsibilities. Both the raw data and TRAC's analysis of that data will inform public debate on government immigration and law enforcement policies.

Defendants claim that records concerning the EID and IIDS databases, including records identifying database table and field names, the code definitions, schema, and software, and technical documentation, are exempt under FOIA Exemption 7(E) because their disclosure will

leave the databases susceptible to a cyber-attack. But defendants' theory of withholding is untethered from the text of Exemption 7(E), as defendants have not demonstrated that any of the records they seek to withhold would reveal techniques, procedures, or guidelines for law enforcement investigations or prosecutions, and risk of a database breach is not the sort of circumvention of the law that the exemption seeks to avoid. Accepting defendants' arguments would enable the government to withhold information about the structure and contents of databases (information necessary to understanding the underlying data and that, if withheld, would be tantamount to withholding that data) as long as those databases had some nexus to law enforcement, providing what amounts to a blanket FOIA exemption for records Congress has given no indication of a desire to exempt. In any event, disclosure of the requested records does not pose any threat to the security of defendants' databases, and thus there is no reasonably expected risk of attack. Moreover, defendants have withheld certain technical documentation for these databases without satisfying their threshold burden to demonstrate that the documentation was compiled for law enforcement purposes.

Defendants have not identified any FOIA exemption that applies to their withholding of the data extracts and snapshots that Long and Burnham requested, and therefore must disclose these records. Rather, defendants base their withholding on the grounds that they lack the technology to produce these extracts in a format that is severable from the databases in which they reside. They contend that disclosure of these records would necessitate the construction of a new database that could provide these extracts in a severable format. Defendants also assert that, even if they were able to produce the extracts, they lack the technical and human resources necessary to review the data and make appropriate redactions of the data pursuant to FOIA exemptions, although they identify no FOIA exemptions they believe would apply. Defendants'

arguments are belied by the facts that they regularly disclose extracts and snapshots from the EID and IIDS to other agencies and have disclosed such records (with and without redactions) to TRAC in response to other FOIA requests.

Finally, defendants have not searched adequately for all records responsive to Long and Burnham's request. Their motion papers make no mention of having searched for certain records (nor do defendants contend that they are withholding those records pursuant to any FOIA exemptions). Defendants also did not search all file systems that contain responsive records. Further underscoring the deficiency of their search, defendants neglected to search any CBP records.

Long and Burnham do not challenge defendants' withholdings of names, email addresses, and phone numbers of federal employees and third parties in records identified in their Vaughn indices pursuant to Exemptions 6 and 7(C). Defendants do not contend that this information cannot reasonably be segregated from non-exempt portions of responsive records.

The Court should deny defendants' motion for summary judgment, grant plaintiffs' motion for summary judgment, and order defendants to disclose all requested records that are not exempt and to conduct an adequate search for all responsive records.

BACKGROUND

I. ICE's Enforcement Integrated Database and Associated Data Repositories

ICE owns and operates the Enforcement Integrated Database (EID), in which "information related to the investigation, arrest, booking, detention, and removal of persons" whom ICE and CBP encounter during immigration and law enforcement investigations and

operations is recorded and maintained. Patterson Declaration ¶ 2 & Ex. A at 2.[1] Several Department of Homeland Security (DHS) components, including defendants' agents and officers, use software applications known as the "ENFORCE applications" to "create[], update[], and access[]" EID records. Patterson Decl. Ex. A at 2, 5. Each ENFORCE application records information about a person that corresponds to a "particular phase of the immigration enforcement process … (arrest, booking, detention, or removal)." *See id.* at 2. The information recorded about a particular individual creates a comprehensive personal profile, comprising data such as height, weight, eye color, birth, education, travel, and even information about the individual's relatives, and also provides a detailed history concerning his or her encounters with immigration or other law enforcement officials. *See id.* at 7-9 (outlining types of information recorded and maintained in the EID). This information is used to assist DHS in deporting people who are in the United States illegally, arresting people who violate federal immigration, customs, or national security laws, conducting background checks of people whose immigration status matters for employment purposes, and tracking criminal or civil proceedings involving individuals apprehended by defendants. *See id.* at 11.

ICE also operates other databases—the EID Datamart, the ENFORCE Alien Removal Module (EARM) Datamart, and the ICE Integrated Decision Support (IIDS) System—that contain subsets of the EID data. *Id.* at 6. Specifically, the EID Datamart contains information concerning arrests and investigations, the EARM Datamart contains information related to past

[1] Exhibit A to the Patterson declaration is ICE's Privacy Impact Assessment (PIA) for the EID. As the Department of Homeland Security's website provides, a PIA is an "assessment of the privacy impact of any substantially revised or new Information Technology System" that is mandated by the E-Government Act of 2002, Pub. Law 107-347, 116 Stat. 289 (Dec. 17, 2002). *See* Department of Homeland Security, *Privacy Office – Privacy Impact Assessments (PIA)*, http://www.dhs.gov/privacy-office-privacy-impact-assessments-pia. Much of the factual information set forth herein is taken from the PIA for the EID.

and pending removal proceedings (including information concerning an individual's detention), *id.* at 7, and the IIDS "concentrates on person and event data for use by ICE." Long Declaration ¶ 7 & Ex. F at1. CBP separately maintains a data warehouse that contains a subset of the EID data related to individuals who are arrested or prosecuted for violations of federal laws within the agency's enforcement authority. *Id.* at 2. These databases contain "continuously updated snapshot[s] of selected EID data," and are queried instead of the EID itself both to ensure the integrity of the data maintained in the EID and the performance of the EID and ENFORCE applications. Patterson Decl. ¶ 2 & Ex. A at 6-7.

II. How Data from the Databases Are Used

A number of federal agencies, including ICE, use EID data to support their functions. ICE uses EID data to "obtain information on previously arrested subjects in support of current investigations or prosecutions" and to manage "detention facility assignments, bed space, [the] transfer of detainees among detention facilities, and [the] coordination of travel to remove aliens from the United States." *Id.* at 14. Other DHS components, such as United States Citizenship and Immigration Services and the Coast Guard, rely on EID data concerning the immigration and criminal histories of individuals in decisionmaking regarding immigration benefits and in maritime enforcement activities, respectively. *Id.* at 14-15. The Federal Bureau of Investigation, the Department of State, and the Social Security Administration likewise rely on EID data provided by ICE on a periodic basis to support various agency functions. *Id.* at 20-21. ICE also furnishes EID data to foreign embassies and consulates to comply with obligations under international treaties. *Id.* at 21.

Significantly, because data in the EID "constitute[] the official records of [DHS immigration and law enforcement investigations and operations]," *id.* at 6, the data underlie

many of the government's immigration policy decisions. ICE generates statistical reports using the EID data to inform DHS and ICE management of its immigration and law enforcement activities, *id.* at 14, and to aid agency management "in setting and evaluating law enforcement strategies, target goals, training and development activities, hiring and staffing, and system enhancement efforts." *Id.* at 15. At the request of the House Committee on Homeland Security, the Government Accountability Office (GAO) compared CBP's deployment of resources at Arizona's border with Mexico to deployments at other locations along the southwest border, Patterson Decl. ¶ 3 & Ex. B at 2, by, in part, analyzing EID data over a five-year period, *id.* at 45 (using EID data on apprehensions and seizures to "assess trends in … data [CBP] uses to inform changes in the status of border security across the southwest border and in the Tucson sector"). That analysis informed GAO's recommendations that the agency develop milestones and timeframes by which to measure its performance in implementing a new border security plan intended to deploy resources to manage risks. *Id.* at 39-40. ICE also furnishes EID data to Congress in fulfillment of statutory mandates. *See* Patterson Decl. ¶ 4 & Ex. C at 1-2 (extracting data from IIDS to provide a report on the deportation of parents of U.S.-born children pursuant to the FY 2012 DHS Appropriations Act, Pub. L. No. 112-74, 125 Stat. 786 (Dec. 23, 2011)).

III. Access to the Databases Is Limited To Ensure Its Security.

As set forth in the Privacy Impact Assessment for the EID, ICE has expended considerable effort to ensure the security of the data in the EID and its associated databases. DHS determines who may access the databases through a user account—and even conducts background checks on each prospective user—and decides what data each user can read and edit. Patterson Decl. ¶ 2 & Ex. A at 13. The agency audits both system operation and usage to detect unauthorized access. Patterson Decl. Ex. A at 13.

The EID database has no publicly available electronic interface. *Id.* at 15 ("EID does not electronically interface with commercial or public sources or systems directly."). Nor do entities outside of DHS have direct access. *Id.* at 22. Instead, ICE furnishes EID data electronically "routinely and … in bulk" to other agencies by "external interface connections in encrypted form" that require ICE to establish user accounts and execute a security agreement with the receiving agency. *Id.* Other agencies receive electronic data extracts from the EID that are uploaded by ICE to a secure file transfer protocol (FTP) server. *Id.* at 20-21. For entities that lack the capability to exchange data through an electronic interface, ICE sends EID data in an encrypted email or on an encrypted DVD/CD that is delivered by a carrier service. *Id.* at 22.

ICE employs a number of "physical, technical, and administrative controls" to mitigate the risks of unauthorized access to the EID and ENFORCE applications. *Id.* at 28. These measures include, among other things, locking users out of sessions for inactivity, locking users out of their accounts after three failed attempts to access the system, implementing firewalls to protect network connections, regularly reviewing audit trails to detect unauthorized use or misuse, and requiring security training for authorized users. *Id.* Notably, the Privacy Impact Assessment does not mention the risk of unauthorized access to the EID by the public.

IV. Plaintiffs' FOIA Requests and Defendants' Responses

Plaintiffs Susan B. Long and David Burnham are the co-directors of TRAC, a Syracuse University research center that gathers information about the functioning of federal law enforcement and regulatory agencies, analyzes the data, and publishes reports. Long Decl. ¶ 2. Specifically, TRAC seeks to provide comprehensive information about the staffing, spending, and enforcement activities of the federal government. *Id.* TRAC also makes data compilations and tools for analyzing data available to others, including Congress, journalists, public interest

groups, scholars, and members of the public. *Id.* TRAC data and studies have been cited by congressional leaders and news organizations in debates over gun control, tax policy, immigration, terrorism, and other law enforcement issues. *Id.* Plaintiffs frequently use FOIA to obtain data from government agencies. *Id.* ¶ 3.

As part of TRAC's ongoing efforts to make information about federal enforcement of immigration laws readily accessible to the public, plaintiffs submitted a number of FOIA requests to ICE and CBP regarding the EID and associated databases, seeking information about and data from these databases. Long Decl. ¶ 3. As explained above, the EID contains official records of defendants' investigative, enforcement, and operations activities, and that data in turn informs the government's immigration policy decisions. *Id.* Disclosure of the types of information recorded in these databases, as well as extracts of subsets of actual data, will ensure that the public is able to participate more effectively in immigration policy debates, which implicate issues as diverse as education, employment, and public safety. *Id.*

The following FOIA requests form the basis of this lawsuit:

October 13, 2010: Plaintiffs submitted a request to ICE for a "complete set of documentation on the [EID]," including records identifying the database tables and fields within each table, records defining each code used in recording data in the EID, records of the EID's database schema,[2] and records identifying the EID's software and the version number of that software. Pineiro Decl. Exh. 1. ICE responded by administratively closing the request on the basis that it had supposedly disclosed the database schema and codes in response to a prior FOIA

[2] The request described the schema as "a specific class of records included in a database system that sets forth how the database tables are interlinked." Pineiro Decl. Exh. 1; *accord* Miller Decl. ¶ 11 ("[T]he schema defines the tables, the fields in each table, and the relationships between fields and tables.").

request by plaintiffs, and ICE later failed to respond after plaintiffs' appeal explaining why this request was not duplicative of prior requests was remanded for an additional search. *Id.* Exhs. 4-5; Long Decl. ¶ 4.

In this action, ICE asserts that it searched its system lifecycle management (SLM) repository for records responsive to this request and has withheld these in full pursuant to FOIA Exemptions 6, 7(C), and 7(E). Wilson Decl. at 5-6. These withholdings are purportedly listed on a supplemental Vaughn index that defendants filed on August 12, 2014. *See* Wilson Decl. at 6; Patterson Decl. ¶ 5 & Exh. D.[3] ICE also withheld, pursuant to Exemption 7(E), what it referred to as metadata (information responsive to plaintiffs' request for the names of the database tables and fields, and code definitions), as well as the database schema and information about the software used to construct the EID. Miller Decl. ¶¶ 6, 10, 20.

October 18, 2010: Long and Burnham submitted a request to ICE for a "complete set of documentation on the [IIDS]," including records identifying the database tables and fields of information stored in each table, records defining each code used in recording data in the IIDS, records of the IIDS database schema, and records identifying the IIDS's software and the version number of that software. Pineiro Decl. Ex. 8. During the administrative process, ICE disclosed 97 pages of documents with redactions pursuant to FOIA Exemption 7(E). *Id.* Ex. 10. Long and Burnham appealed, challenging the application of Exemption 7(E), the adequacy of ICE's search, and ICE's failure to disclose the entire document of which the 97 pages purportedly were a part. *Id.* Ex. 11. On appeal, ICE affirmed those withholdings and remanded the request for additional searches and re-processing of certain records. *Id.* Ex. 13.

[3] Defendants filed a 10-page supplemental Vaughn index with unnumbered entries. A numbered version created by plaintiffs is attached to counsel's declaration, and this memorandum will refer to various entries by those numbers for the Court's convenience.

In this action, ICE asserts that it searched its SLM repository for additional records and withheld all responsive records in full pursuant to FOIA Exemptions 6, 7(C), and 7(E). Wilson Decl. at 5-6. ICE purports to list those withheld records on the supplemental Vaughn index, *see id.* at 6; Patterson Decl. ¶ 5 & Exh. D. Further, ICE has described the redactions it made, also pursuant to Exemptions 6, 7(C), and 7(E), to the 97 pages it disclosed during the administrative proceedings on a Vaughn index it filed on June 18, 2014 ("first Vaughn index"). Pineiro Decl. ¶ 44 & Exh. 26. ICE has also withheld metadata, schema, and software information pursuant to Exemption 7(E). Miller Decl. ¶ 20.

September 21, 2012: Long and Burnham submitted two FOIA requests to ICE. In the first, they sought records "identifying any extracts and 'snapshots' prepared from the [EID] over the last 12 months" ("extract identification records"). Pineiro Decl. Exh. 14. They also sought records identifying the frequency with which the extracts were prepared, who was responsible for preparing each extract, the recipients of those extracts, and the EID system time required to prepare each extract ("extract preparation records"). *Id.* 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). *Id.* Exh. 15. Long and Burnham appealed both the withholdings pursuant to Exemption 7(E) and the adequacy of ICE's search, noting that the nine pages appeared to be summaries of various ICE records—rather than the records themselves—that were compiled specifically to respond to their request. *Id.* Exh. 16. They also appealed ICE's failure to disclose any extract identification or extract preparation records. *Id.* ICE remanded the request for additional searches for responsive records, and did not address the appeal of the withholdings under Exemption 7(E). *Id.* Exh. 18.

In the second request, Long and Burnham sought the most current extract of data from the EID and loaded into IIDS "existing at the time" ICE processed the request. Pineiro Decl. Ex. 19. ICE did not respond to the request before this action was filed. Long Decl. ¶ 9.

February 25, 2013: Long and Burnham submitted a FOIA request to both ICE and CBP seeking "the most current snapshot existing at the time this request is processed" of "information in the [EID that] 'is replicated to … [the] CBP Data warehouse.'" Pineiro Decl. Ex. 21. ICE responded that it had no responsive records. *Id.* Ex. 22. CBP did not respond to the request. Long Decl. ¶ 10.[4]

February 26, 2013: Long and Burnham submitted two FOIA requests seeking the most current extracts of EID data "existing at the time this request is processed" for the EARM Datamart (addressed only to ICE) and the EID Datamart (addressed to both ICE and CBP). Pineiro Decl. Exh. 23. Defendants did not respond to either request. Long Decl. ¶ 11.

V. Defendants' Withholdings

In their motion for summary judgment, defendants invoke Exemption 7(E) as the basis for withholding metadata, schema, and software records concerning the EID and IIDS databases (requested by plaintiffs on October 13 and 18, 2010), on the basis that disclosure "would expose ICE's sensitive law enforcement data systems to outside entities, and allow individuals, companies, or foreign governments to gain unauthorized access to the contents of those systems." Pineiro Decl. ¶¶ 15, 24; *see also* Miller Decl. ¶ 25 (stating that disclosure of metadata and other law enforcement database information requested "*could* expose ICE's sensitive law enforcement data systems" to the same risk described in the Pineiro declaration) (emphasis

[4] Long and Burnham did not appeal ICE's denial. Long Decl. ¶ 10. Accordingly, they allege Count 5 of their complaint (which is based on their February 25, 2013, request) against CBP only.

added). Defendants also claim Exemption 7(E) as the basis for withholding portions of 97 pages disclosed in response to the October 18, 2010, request and portions of nine pages disclosed in response to the September 21, 2012, request for records concerning EID data extracts and data snapshots because "release of certain information relating to the structure of these systems" could facilitate unauthorized access to the databases. *See* Pineiro Decl. ¶ 47. And although defendants remanded the first of the September 21, 2012, requests to conduct additional searches after Long and Burnham pointed out that defendants had failed to disclose the extract identification or extract preparation records, *see* Pineiro Decl. Exh. 18, defendants' motion papers make no mention of these records.

Defendants further contend that they lack the technology to produce either snapshots of data in the EID or the extracts of EID data loaded into the IIDS, CBP Data warehouse, EARM Datamart, or EID Datamart. Wilson Decl. at 9. Moreover, they assert that there are no records responsive to the requests for snapshots "from the day of the subject FOIA request," Defs.' Mem. at 12, because the data in the associated databases are replaced by updated extracts from the EID every 48 hours, and the older data extracts are not retained.[5] Defs.' Mem. at 12 (citing Wilson Decl. at 4). Defendants further claim that, even if they had the capability to disclose the data extracts and snapshots, they lack the technology necessary to redact information, Wilson Decl. at 9, even though they have not claimed that any FOIA exemption applies to plaintiffs' requests for extracts or snapshots.

[5] The Wilson declaration describes the updating and replacement of data extracts every 48 hours only with respect to the IIDS database, *see* Wilson Decl. at 4. Defendants' memorandum, however, suggests that extracts of EID data loaded into the other data repositories are not retained either. *See* Defs.' Mem. at 11-12.

STANDARD OF REVIEW

Summary judgment is appropriate when "there is no genuine dispute as to any material fact," Fed. R. Civ. P. 56(a), with all reasonable inferences to be drawn in favor of the non-movant. *Burka v. Dep't of Health & Human Servs.*, 87 F.3d 508, 514 (D.C. Cir. 1996).[6] In FOIA cases, the agency bears the burden of proving that a requested record is exempt from disclosure. *Pub. Citizen, Inc. v. OMB*, 598 F.3d 865, 869 (D.C. Cir. 2010) (citation omitted). This Court reviews the agency's claimed exemptions *de novo*. 5 U.S.C. § 552(a)(4)(B). The requested records must be disclosed "where the government does not carry its burden of convincing the court that one of the statutory exemptions apply." *Goldberg v. U.S. Dep't of State*, 818 F.2d 71, 76 (D.C. Cir. 1987).

ARGUMENT

FOIA is intended to "pierce the veil of administrative secrecy and to open agency action to the light of public scrutiny," *Dep't of Air Force v. Rose*, 425 U.S. 352, 361 (1976) (citation omitted), by ensuring "that the public has access to all government documents, subject to only nine specific limitations, to be narrowly interpreted." *Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 862 (D.C. Cir. 1980). At issue here are defendants' withholdings under

[6] Local Rule 7(h) requires a party moving for summary judgment to include a statement of material facts as to which that party contends there is no genuine issue, thus affording the opposing party the opportunity to dispute those facts. *See Boone v. MountainMade Found.*, -- F. Supp. 2d --, 2014 WL 4096477, at *4 (D.D.C. Aug. 20, 2014). Defendants have not provided any such statement. This omission should bar the Court from treating the government's factual contentions concerning such matters as risks of cyber-attacks and the burdens of producing and redacting data extracts as undisputed even if the plaintiffs had not, in the accompanying declarations and exhibits, demonstrated that the deficiencies and inconsistencies in the defendants' factual contentions are so severe that there is in actuality no genuine dispute as to the plaintiffs' positions on these matters.

Exemption 7(E), their withholdings of the various data snapshots and extracts, and the adequacy of their search.

I. Defendants Have Not Demonstrated that Exemption 7(E) Justifies Withholding Any Records Related to the Databases.

An agency may withhold "records or information compiled for law enforcement purposes to the extent release of such records '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.'" *Citizens for Responsibility & Ethics in Wash. v. DOJ*, 746 F.3d 1082, 1101-02 (D.C. Cir. 2014) (citing 5 U.S.C. § 552(b)(7)(E)) ("*CREW*"). Defendants have failed to demonstrate that Exemption 7(E) applies to any of the withheld records.

A. Disclosure of the EID and IIDS Metadata, Schema, and Software Records Will Not Reveal Techniques, Procedures, or Guidelines.

Defendants concede that the EID and IIDS metadata—here, the names of the database tables and information fields within each table and the codes used to record information within the databases—and the schema and software records are not themselves "techniques and procedures … or … guidelines for law enforcement investigations or prosecutions." 5 U.S.C. § 552(7)(E); *see* Defs.' Mem. at 21 (describing the FOIA requests as seeking "*only* … fields, codes, database tables, and database schema") (emphasis added). And they do not even argue that disclosure of these records would in any way reveal any such techniques, procedures, or guidelines.

Rather, defendants contend that disclosure of these records will "allow individuals to access [ICE's] law enforcement databases, including its investigative files, manipulate data within those databases, and launch a full scale cyber-attack" against ICE. Defs.' Mem. at 21. The

information contained in those databases, defendants aver, was obtained *using* "certain law enforcement techniques and methods." Pineiro Decl. ¶ 50. Defendants do not contend, however, that disclosure of the information contained in the databases would reveal the techniques, procedures, or guidelines themselves, nor are there any facts in the record that would allow this Court to draw reasonable inferences that such disclosure would occur. Under the plain language of Exemption 7(E), the Court need not consider the possibility of circumvention of the law unless the risk of circumvention results from "such disclosure"—i.e., disclosure of "techniques," "procedures," or "guidelines." 5 U.S.C. § 552(b)(7)(E). On this basis alone, the records should be released. *See Strunk v. Dep't of State*, 845 F. Supp. 2d 38, 47 (D.D.C. 2012) (denying CBP's motion for summary judgment on Exemption 7(E) claim because agency failed to demonstrate that records would disclose any law enforcement techniques, procedures, or guidelines).

Moreover, defendants have failed to clear "the low bar for … withholding" under Exemption 7(E) because they have not provided any information about what the techniques, procedures, or guidelines that supposedly underlie the records at issue might be. *See CREW*, 746 F.3d at 1102 (requiring agency to "at least provide *some* explanation of what procedures are involved and how they would be disclosed"); *Blackwell v. FBI*, 646 F.3d 37, 42 (D.C. Cir. 2011) (holding that agency satisfied its burden by identifying "[f]orensic examination procedures" and "methods of data collection, organization, and presentation contained in [certain] reports" as techniques and procedures at risk of disclosure). Thus, the Court should reject defendants' conclusory contention that "Exemption (b)(7)(E) was created to protect the exact information [p]laintiffs will be able to access if responsive information to the subject FOIA requests is produced." Defs.' Mem. at 24.

B. Risk of a Database Breach Is Not a Cognizable Harm Under Exemption 7(E).

Defendants assert that the release of the requested records will place ICE at "risk of a cyber-attack" because knowledge of the schema "can be used by a malicious intruder to construct an attack that targets the formats and characteristics of the database," Defs.' Mem. at 23 (citing Miller Decl. ¶ 11), and knowledge of the metadata "can [be] use[d] to construct an attack targeting the data formats and data elements within the database," *id.* at 22 (citing Miller Decl. ¶ 10). Defendants contend that "[k]nowing the type and version of the database used by a Web application allows an attacker to craft database specific attacks." Miller Decl. ¶ 18.

Defendants fail to meet their burden of demonstrating "logically how the release of [the requested] information might create a risk of circumvention of the law." *Mayer Brown LLP v. IRS*, 562 F.3d 1190, 1194 (D.C. Cir. 2009) (citation and internal quotation marks omitted). Although 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). Rather, the exemption allows an agency to withhold techniques, procedures, and guidelines that it uses to enforce particular laws, either by investigation or prosecution of a violation, if disclosure of those techniques, procedures, or guidelines would allow an individual to circumvent *those* laws. Defendants' reading of Exemption 7(E) thus fails for three reasons. First, it excises the statutory text that requires the disclosure of "such [techniques, procedures, or guidelines]" to result in a risk of circumvention of the law. Second, defendants replace the word "circumvention"—the consequence of disclosure that the statute seeks to avoid and that establishes the relationship between the techniques, procedures, and guidelines in the first clause and the law in the second clause—with the wholly distinct word "violation." Third, defendants' interpretation divorces "the law" from the rest of the statutory text to support their theory that the exemption applies

whenever disclosure of records could risk violation of *any* law.[7] Defendants' atextual application of Exemption 7(E) to these records should be rejected.

None of the cases that defendants cite supports their attempt to apply Exemption 7(E) to records whose disclosure allegedly could result in a violation of a law wholly unrelated to the laws to which the withheld techniques, procedures, or guidelines relate. In *Blackwell*, the court affirmed withholdings pursuant to Exemption 7(E) of records outlining forensic examination procedures for computers because disclosing that information would "expos[e] computer forensic vulnerabilities" to "individuals who seek to utilize computers in violation of laws." 646 F.3d at 42. Likewise, in *Public Employees for Environmental Responsibility v. U.S. Section, International Boundary & Water Commission*, 740 F.3d 195, 205 (D.C. Cir. 2014) (*PEER*),[8] the court held that Exemption 7(E) applied to emergency action plans for certain dams that outlined guidelines for detecting the cause of a dam failure and security precautions for law enforcement personnel in case of an emergency because disclosure could allow terrorists or criminals to "use the information … to thwart rescue operations following a dam failure or to obstruct attempts to investigate the source of such a failure." *See also Showing Animals Respect & Kindness v. U.S. Dep't of Interior*, 730 F. Supp. 2d 180, 200 (D.D.C. 2010) (approving application of Exemption 7(E) to records that would "reveal specific details of surveillance techniques, including

[7] Further, defendants incorrectly suggest that they are entitled to a "categorical exemption to all of the information," Defs.' Mem. at 25, presumably for "techniques and procedures used in law enforcement investigations or prosecutions," citing the district court's decision in *Public Employees for Environmental Responsibility v. U.S. Section of International Boundary & Water Commission*, 839 F. Supp. 2d 304, 327 (D.D.C. 2012). On appeal of that case, however, the D.C. Circuit clarified that the "risk circumvention of the law" modifier applies "both to records containing guidelines and to records containing techniques and procedures." *Pub. Employees for Envtl. Responsibility v. U.S. Section, Int'l Boundary & Water Comm'n*, 740 F.3d 195, 205 n.4 (D.C. Cir. 2014) (citing *Blackwell*, 646 F.3d at 41-42).

[8] Defendants cite to the district court decision in *PEER*. *See* Defs.' Mem. at 25.

equipment used and location and timing of use," which would aid trespassers and poachers in national wildlife refuges in evading surveillance); *Tunchez v. DOJ*, 715 F. Supp. 2d 49, 56 (D.D.C. 2010) (finding the withheld information concerning the FBI's assessment of techniques and procedures used to investigate the plaintiff would be "useful [to other investigative targets] in evading detection"); *Burke v. DOJ*, Civ. No. 96-1739, 1999 WL 1032814, at *8 (D.D.C. Sept. 30, 1999) (finding that "potential and actual criminals might have used" redacted information concerning the FBI's ratings of the efficacy of methods such as informants, photographs, surveillance, and telephone toll coverage "to develop countermeasures" against those techniques).

Notably, defendants do not argue that disclosure of the EID and IIDS metadata, schema, and software records—assuming that they even reveal techniques, procedures, or guidelines, which they do not—will enable individuals to use knowledge of ICE's enforcement methods to evade arrest, detention, or deportation for violations of the federal immigration or criminal laws to which ICE's supposed techniques, procedures, and guidelines relate. *Cf. Mayer Brown*, 562 F.3d at 1193-94 (withholding records of IRS settlement strategies and assessments of litigation hazards because disclosure would "affect[] the cost-benefit analysis of potential [tax] evaders" by "mak[ing] evasion an appealing gamble" and would help a "potential evader … know how to best structure an evasion so as to avoid the maximum enforcement efforts of the IRS."); *Schnapp v. U.S. Citizenship & Immigration Servs.*, -- F. Supp. 3d --, 2014 WL 4436925, at *2 (D.D.C. Sept. 9, 2014) (finding disclosure of law enforcement records "could enlighten asylum applicants with criminal backgrounds about what sort of law enforcement information (from which databases) is consulted by [the agency] during adjudication of a pending asylum application—and, of course, by logical inference, what sort of information is not consulted."). The risk of a

database breach posed by disclosure of these records, which do not convey techniques, procedures, or guidelines concerning database security, is not the type of harm against which Exemption 7(E) is intended to protect.

But even if the harm that defendants fear were within the realm of Exemption 7(E), the risk is not one that can be "reasonably expected," *Blackwell*, 646 F.3d at 42, to result from the disclosure. Defendants contend that an intruder will be able to use database table and field names and schema information to construct a type of attack known as an injection attack using Structured Query Language (SQL), a programming language used to manage data within a database. Miller Decl. ¶¶ 16, 19. Specifically, defendants assert that an intruder with knowledge of specific data formats and data elements within the EID or IIDS could access and modify or delete data within those databases by sending "malicious SQL commands" through a web application that transmits information to the databases. *See* Miller Decl. ¶ 10. According to defendants, an intruder "can trick the web application into forwarding a malicious query to the database" that incorporates the actual data element and "result[s] in a database error, which can allow the attacker to modify data, delete data or view data that would not ordinarily be made available." *Id.*

This fear is unfounded. The type of cyber-attack that defendants theorize disclosure of these records may threaten would require a direct connection to the databases. Clark Decl. ¶ 13; *see also* Miller Decl. ¶ 10 (contemplating an attack using "a web application"). As ICE's Privacy Impact Assessment for the EID makes clear, the database is not publicly accessible, nor do agencies outside of DHS have access to the databases. Clark Decl. ¶ 13 (citing Patterson Decl. ¶ 2 & Exh. A at 15, 22). Thus, any threat of attack could be posed only by defendants' employees and contractors with a direct connection to the EID, who already can access the

names of the database tables and fields and schema. Clark Decl. ¶ 13. Disclosure of the requested records to the public poses no increased threat to defendants' databases. *Id.*

Further, defendants' theory is premised on an implicit assumption that defendants do not follow accepted best practices for data security. *See* Clark Decl. ¶ 14. These best practices include the implementation of firewalls that would prevent a direct connection to the database by the public (even if there were a publicly available web interface, which there is not) and the use of security protocols designed to prevent either a user from altering any instructions a database executes or a database from executing any query without first validating the commands. *See id.* That assumption is belied by ICE's statements regarding its extensive security precautions, including firewalls to protect the EID from unauthorized intrusions and network security monitoring that "proactively stop[s] and captur[es] malicious code." *Id.* (citing Patterson Decl. ¶¶ 2, 6 & Exh. A at 27-28; Exh. E at 78). Thus, disclosure of the metadata and schema does not pose any new threat to the security of the databases, and will not create a risk of attack. Clark Decl. ¶ 15. Indeed, ICE administratively closed plaintiffs' October 13, 2010, FOIA request on the grounds that it had disclosed the EID schema in response to an earlier FOIA request by plaintiffs before granting plaintiffs' appeal and remanding for a search for updated schema. Pineiro Decl. Exh. 4; Long Decl. ¶ 12 & Exh. G; *see also* Long Decl. ¶¶ 13-14 & Exhs. H-I (disclosures of IIDS metadata and software information in response to October 18, 2010, request). Defendants' previous assertion that they had disclosed the requested information suggests that defendants' claimed belief that disclosure of these records will render the databases vulnerable to a breach reflects a litigation strategy rather than a genuine fear that they are unable to secure their systems.

Moreover, defendants' rationale for withholding this information is premised on a principle of database security known as "security through obscurity"—the notion that a computer system is harder to attack if details concerning the system are kept secret—that has long been rejected as a best practice. Clark Decl. ¶ 16. Network security experts now understand that disclosing an algorithm to be used by a server to encrypt data, thus rendering that algorithm susceptible to testing prior to deployment, is a far superior method of data security than keeping the encryption algorithm a secret and hoping that it will never be discovered and attacked. *Id.* Indeed, the information security standards promulgated by the National Institute for Standards and Technology for federal government networks make clear that "[s]ystem security should not depend on the secrecy of the implementation or its components." Clark Decl. ¶ 16 (quoting Karen Scarfone, Wayne Jansen, & Miles Tracy, *Guide to General Server Security: Recommendations of the National Institute of Standards and Technology*, Special Pub. 800-123, at 2-4 (July 2008)).[9] Thus, defendants' contention that withholding the database software records is justified by the possibility that disclosure will "allow[] an attacker to craft database specific attacks" and that withholding the schema is permissible because disclosure would allow an "attacker … [t]o correctly extract data from a database," Miller Decl. ¶ 18, contravenes best practices for data security. Clark Decl. ¶ 17. Indeed, defendants' comparison of knowledge of the database metadata and schema to knowledge of the combination to a safe, Miller Decl. ¶ 11, is false. Rather, knowledge of the metadata and schema is analogous to knowledge of the type of combination lock on a safe located in an inaccessible facility, which poses no increased risk that the safe's contents will be accessed by an intruder. Clark Decl. ¶ 18. Because there is no public

[9] *Available at* http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf.

or external direct connection to the EID, disclosure of the software records poses no threat and creates no viable risk of an external attack on defendants' databases. Clark Decl. ¶¶ 12-15.

C. Defendants Have Not Sustained Their Burden of Demonstrating that 7(E) Applies to Any of the Records Listed in the Vaughn Indices.

Defendants are withholding in full other records, listed in their supplemental Vaughn index, that were found in their SLM repository and that they contend are responsive to the October 13 and 18, 2010, FOIA requests for a "complete set of documentation" on the EID and IIDS databases. Wilson Decl. at 6. In addition, defendants' first Vaughn index lists redactions of data field names and identification of law enforcement systems that interact with the EARM Datamart in documents disclosed during the administrative process in response to the October 18, 2010, and the September 21, 2012, FOIA requests. *See* Pineiro Decl. Ex. 26 (all entries). Defendants have failed to demonstrate that they are entitled to withhold any of these records.

1. The Records in the Supplemental Vaughn Index Are Not Law Enforcement Records.

As a preliminary matter, although there is no prescribed format for a Vaughn index, *Neuman v. United States*, -- F. Supp. 3d --, 2014 WL 4922584, at *6 (D.D.C. Sept. 30, 2014), a Vaughn index must "enable the court and the opposing party to understand the withheld information in order to address the merits of the claimed exemptions." *Judicial Watch, Inc. v. FDA*, 449 F.3d 141, 150 (D.C. Cir. 2006). The index should "provide a relatively detailed justification, specifically identifying the reasons why a particular exemption is relevant and correlating those claims with the particular part of a withheld document to which they apply," *Morley v. CIA*, 508 F.3d 1108, 1122 (D.C. Cir. 2007) (citation and internal quotation marks omitted), particularly where, as here, multiple exemptions are applied to the same record.

Defendants' supplemental Vaughn index falls well short of this standard. None of the entries identifies the database—EID or IIDS—to which the records relate, making it difficult to determine whether the records listed even are responsive to plaintiffs' requests. And for those entries for which multiple exemptions are claimed, defendants have made no attempt to correlate those exemptions with the portions of the records to which the exemptions are applied. *See, e.g.*, Patterson Decl. ¶ 5 & Ex. D at Entry Nos. 68, 71, & 74 (failing to explain why Exemptions 6 and 7(C) apply, or to which portions of the records Exemption 7(E) applies). Nor have defendants demonstrated why any non-exempt portions of the records cannot be reasonably segregated and disclosed. *See Johnson v. Executive Office for U.S. Attorneys*, 310 F.3d 771, 776 (D.C. Cir. 2002) (noting that it is the "agency's obligation to show with 'reasonable specificity' why a document cannot be further segregated." (citation omitted)).

Even accepting defendants' descriptions at face value, none of the records listed in the supplemental Vaughn index satisfies the threshold requirement of Exemption 7(E) that the records were "compiled for law enforcement purposes." *PEER*, 740 F.3d at 203 (citing 5 U.S.C. § 552(b)(7)). To establish that this requirement is satisfied, defendants must show "a rational 'nexus between the investigation and one of the agency's law enforcement duties,' … and a connection between an 'individual or incident and a possible security risk or violation of federal law.'" *Campbell v. DOJ*, 164 F.3d 20, 32 (D.C. Cir. 1998) (citation omitted). The Supreme Court and the D.C. Circuit have construed "law enforcement" to refer to both "investigating and prosecuting individuals *after* a violation of the law," *PEER*, 740 F.3d at 203, and to "proactive steps designed to prevent criminal activity and to maintain security." *Id.* (quoting *Milner v. Dep't of Navy*, 131 S. Ct. 1259, 1272 (2011) (Alito, J., concurring)). Records that are compiled

originally for one purpose may nonetheless "fall within Exemption 7 if they are later assembled for law enforcement purposes." *Milner*, 131 S. Ct. at 1273 (Alito, J., concurring).

As the Privacy Impact Assessment for the EID provides, the EID exists in "four technically discrete environments: development, operational, testing, and training," Patterson Decl. ¶ 2 & Exh. A at 6, with the development, testing, and training modules using dummy data rather than "real data … created during DHS immigration and law enforcement investigations and operations." *Id.* Numerous entries on the supplemental Vaughn index make reference to these non-law enforcement functions, and defendants' corresponding descriptions confirm that these records were not compiled originally for law enforcement purposes. *See, e.g.*, Patterson Decl. ¶ 5 & Exh. D at Entry Nos. 3, 39, 47, 53 (training); 14, 27, 32, 40, 57, 71 (development); 19, 30, 51-52 (testing).

Nor is there anything in the record that would allow this Court to infer that the records were "later assembled for law enforcement purposes." *Milner*, 131 S. Ct. at 1273 (Alito, J., concurring). Defendants' only declaration that discusses the supplemental Vaughn index refers the Court to certain paragraphs of other witness declarations for the reasons for withholding records pursuant to Exemption 7(E). *See* Wilson Decl. at 6 (referencing Miller Decl. ¶¶ 20-25 and Pineiro Decl. ¶¶ 40-56). Pineiro's declaration makes no mention of the supplemental Vaughn index, and Miller's declaration attempts to explain the withholdings of only the metadata, schema, and software records that were requested by plaintiffs in October 2010, and not any of the records identified as responsive following defendants' search of their SLM repository. *See* Miller Decl. ¶¶ 6, 20. Moreover, defendants' blanket explanation that "[p]laintiffs' requests sought records from ICE databases that contain information related [to] law enforcement investigations into civil and criminal immigration violations" and the responsive records were

"[t]herefore … compiled for law enforcement purposes," Pineiro Decl. ¶ 49, is too sweeping and conclusory to satisfy defendants' threshold burden under Exemption 7. *See Campbell,* 164 F.3d at 32 (rejecting "claim that anything in an FBI file pertains to an exempt law enforcement purpose.").

2. Disclosure of the Records Listed in Either Vaughn Index Will Not Result in a Risk of Cyber-Attack or Reveal Techniques, Procedures, or Guidelines for Law Enforcement Investigations or Prosecutions.

As explained above, *see* Section I.B, a risk of unauthorized access to the EID and IIDS databases that allegedly would result from disclosure of these records does not satisfy Exemption 7(E) and is not a risk that can reasonably be expected to materialize. Because the EID lacks a publicly available web interface necessary to launch an attack, and defendants' use of firewalls and other measures to prevent unauthorized access provide ample protection against an attack even if there were a publicly accessible web interface, disclosure of any records relating to the databases will not create a new threat to their security and, therefore, creates no risk of attack. Clark Decl. ¶¶ 12-15. Defendants' contentions, therefore, that disclosure of various types of information contained in responsive records would allow an intruder to exploit system vulnerabilities or to time an attack when the system is experiencing an outage, are unavailing. Clark Decl. ¶¶ 20-21 (citing Patterson Decl. ¶ 5 & Exh. D at Entry Nos. 4, 9, 14, 16, 18, 27, 29, 40, 43, 51-52, 71, 74, 82, 86, 89-97, 107-108, 153). Likewise, no risk of an attack can result from disclosure of the names of data fields or the law enforcement systems that interact with defendants' databases. Clark Decl. ¶ 22 (citing Pineiro Decl. Exh. 26).

Moreover, defendants' reasons for withholding are described only in general terms that do not "enable the [C]ourt … to understand the withheld information in order to address the merits of the claimed exemptions." *Judicial Watch,* 449 F.3d at 150. Although defendants may

desire to protect "sensitive information" relating to their database systems, *see, e.g.*, Patterson Decl. ¶ 5 & Ex. D at Entry Nos. 147, 150-152,[10] nothing in the record indicates that any document listed in either Vaughn index reveals techniques, procedures, or guidelines for law enforcement investigations and prosecutions. Because FOIA's exemptions are exclusive and must be "narrowly construed," *Milner*, 131 S. Ct. at 1262 (citation omitted), the Court should deny defendants' motion for summary judgment, grant summary judgment to plaintiffs, and order disclosure of the records or portions of records listed on both Vaughn indices that defendants have withheld pursuant to Exemption 7(E).

II. Because Defendants Have Not Asserted Any Exemption Applicable to the Data Snapshots and Extracts, They Must Disclose These Records.

Under FOIA, an agency may withhold records responsive to a FOIA request "*only* if the information falls within" an exemption. *People for the Ethical Treatment of Animals v. NIH*, 745 F.3d 535, 540 (D.C. Cir. 2014) (*PETA*) (emphasis added). Defendants have not claimed that the withheld data snapshots and extracts from the EID and associated databases[11] fall within the scope of any FOIA exemption. The information, therefore, must be disclosed.

[10] Many of defendants' descriptions of records listed in the supplemental Vaughn index are inadequate. A number of entries state that the records "*can* contain sensitive information," *see, e.g.*, Patterson Decl. ¶ 5 & Exh. D at Entry Nos. 2, 8, 56, 84-85, "*could* provide information that *could* be used," *id.* at Entry No. 52, or "*may* include sensitive comments," *id.* at Entry No. 98 (emphasis added). And other records are withheld on the grounds that their "sensitivity … is unable to be determined because [they are] currently an unreadable file type." *See, e.g.*, *id.* at Entry Nos. 45, 105. These descriptions suggest that defendants have not reviewed these records to determine whether their content falls within any FOIA exemption and should preclude this Court from granting summary judgment in defendants' favor.

[11] Nothing in the record before the Court explains why defendants have not produced a data snapshot from the CBP Data warehouse. Although defendants make fleeting references to the CBP Data warehouse, *see* Wilson Decl. at 7, 9, their declarant is an ICE employee who does not appear to have knowledge of CBP's record systems or technological capabilities. *See* Wilson Decl. at ¶ 1 (detailing employment history at ICE and Treasury Department).

A. As a preliminary matter, defendants misconstrue the FOIA requests as seeking snapshots and extracts "from the date of the FOIA request," Defs.' Mem. at 12, rather than those "existing at the time [the] request is processed," as the requests state. *See* Pineiro Decl. Exhs. 19, 21, 23. *See also Pub. Citizen v. Dep't of State*, 276 F.3d 634, 642-44 (D.C. Cir. 2002) (rejecting agency policy applying date-of-request cut-off date for records responsive to FOIA request). To the extent that defendants' denial of these records is based on the claim that no responsive records exist because the agencies do not retain data snapshots or extracts for more than 48 hours, *see* Defs.' Mem. at 12-13, that denial is improper because defendants have a duty to preserve records that have been requested under FOIA. *See Chambers v. Dep't of Interior*, 568 F.3d 998, 1004 (D.C. Cir. 2009) (denying summary judgment for agency where factual question existed whether agency intentionally destroyed record after it was requested); *see also* 6 C.F.R. § 5.10 (DHS FOIA regulation providing that "[r]ecords will not be disposed of while they are the subject of a pending FOIA request.").

B. Defendants' regular production of extracts and snapshots from the EID and other databases to organizations outside of DHS undermines their argument that ICE lacks the technology to produce the snapshots and extracts because the extraction process "is accomplished via a link established between … two databases" and "does not generate specific extract files." Wilson Decl. at 8. The EID Privacy Impact Assessment describes ICE's capability to produce electronic extracts from the database to external entities, not through a direct connection between two databases, but by uploading the extract files to a secure FTP server, Patterson Decl. ¶ 2 & Exh. A at 20-21, or by sending the file in an encrypted email or on an encrypted DVD/CD. *Id.* at 22. Indeed, one of the documents that defendants have withheld apparently "includes instructions for copying files to and from servers." Patterson Decl. ¶ 5 &

Exh. D at Entry No. 107. And defendants make no attempt to reconcile their claimed inability to produce extracts and snapshots in this case with their prior disclosures of extracts from the EID and IIDS to plaintiffs. *See* Long Decl. ¶¶ 16-19 & Exhs. J-M.

Moreover, defendants' comparison of the more than 6.7 billion rows of EID data to 1.8 million songs on an iPod has no bearing on their technological capability to extract data from the EID or any other database. Hasan Decl. ¶ 11 (citing Wilson Decl. at 7). One purpose of any standard database management software (DBMS) is to facilitate reporting of data by allowing users to query and extract data. *Id.* ¶ 10. Thus, extraction capability is common across standard DBMS packages. *Id.* Unlike an iPod, which consists of a random collection of songs, a database is structured so that data is arranged in tables and rows, and the purpose of DBMS is to manage this data by means of various automated processes that utilize the same SQL commands regardless of the size of the database. *Id.* ¶ 11. Accordingly, extraction of data is accomplished in the same manner whether the database contains five rows of data or 6.7 billion rows. *Id.* By contrast, an iPod consists of a random collection of songs whose management would be difficult and unwieldy in a software application such as iTunes. *Id.* If the equivalent amount of data were in a database, however, management of that data, including any extraction, would not present those difficulties. *Id.*

Thus, defendants' assertion that a new contract costing "hundreds of thousands to millions of dollars" is required to "facilitate the extract process," Wilson Decl. at 9, is baseless. Even assuming a new contract were necessary, which it is not given defendants' ability to furnish extract files even where a direct connection to the EID is unavailable, defendants fail to document any of the costs allegedly involved, and there is reason to believe their estimates may be overstated significantly. In particular, storage devices capable of storing five terabytes of data

can be purchased for just over 200 dollars, Patterson Decl. ¶ 9, far less than the "thousands of dollars" that defendants assert. Wilson Decl. at 9.

Further, defendants' claim that they lack the technology to redact data and would need to hire experts to do so, and that these assertions provide additional reasons why they cannot provide the data extracts and snapshots, *id.*, presumes that they have satisfied their burden under FOIA to justify redaction of the records, which they have not by failing to claim any FOIA exemption that applies to these records. Moreover, defendants' assertion is demonstrably false. Defendants have previously disclosed to plaintiffs extracts from IIDS from which data has been redacted pursuant to Exemption 7(E). Long Decl. ¶¶ 18-19 & Exs. L-M. In light of these prior disclosures, defendants do not explain adequately why responding to plaintiffs' requests here impose such onerous technical and logistical burdens. Redaction likewise is a standard feature common across commercial DBMS packages, and can be accomplished by means of a SQL command regardless of how much data there is in a database. Hasan Decl. ¶ 13. Thus, defendants' comparison of redaction of data in the EID to redaction of song information on an iPod is false. *Id.* ¶ 14.

But even if the burdens were as significant as defendants claim, those burdens would not provide defendants a justification to avoid their obligations under FOIA to disclose a non-exempt record. *See Citizens for Responsibility and Ethics in Washington v. Dep't of Educ.*, 905 F. Supp. 2d 161, 172 (D.D.C. 2012) (observing that, although electronic versions of records must be produced when requested and when the format is readily reproducible, Congress contemplated that agencies at least would produce "hard paper copies of all records requested" (citing 5 U.S.C. § 552(a)(4)(A)). To hold otherwise would allow defendants to exempt wholesale the official records of their activities on the basis of alleged technical infeasibility, contrary to both FOIA's

text and purpose and leading to a result that Congress never intended. Accordingly, the Court should deny defendants' motion for summary judgment, enter summary judgment in plaintiffs' favor, and order disclosure of the extracts and snapshots.

Alternatively, if the Court determines that defendants' assertions regarding the technical infeasibility of producing and redacting extracts and snapshots from their databases, if true, would be adequate to support withholding of these records (despite the absence of any claimed FOIA exemptions and defendants' failure to explain why producing the records in another format is not a feasible option), the Court should deny both parties' motions for summary judgment to allow plaintiffs an opportunity to conduct discovery on this factual issue. "[S]ummary judgment is not available" in FOIA cases "if material facts are genuinely in issue or, though undisputed, are susceptible to divergent inferences bearing upon an issue critical to disposition of the case." *Alyeska Pipeline Serv. Co. v. EPA*, 856 F.2d 309, 314 (D.C. Cir. 1988). Here, plaintiffs 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. If the Court finds that plaintiffs' evidence falls short of justifying a grant of summary judgment in their favor, plaintiffs respectfully request that the Court deny the pending motions for summary judgment and grant plaintiffs leave to take necessary discovery.

III. Defendants' Search Was Inadequate.

FOIA requires an agency to conduct a search for responsive records that is "reasonably calculated to discover the requested documents." *SafeCard Servs., Inc. v. SEC*, 926 F.2d 1197, 1201 (D.C. Cir. 1991). An inadequate search amounts to an improper withholding. *Scaff-Martinez v. Drug Enforcement Admin.*, 770 F. Supp. 2d 17, 21 (D.D.C. 2011) (citation omitted).

An agency is required to search all record systems that are "likely to produce responsive documents." *Oglesby v. Dep't of Army*, 920 F.2d 57, 68 (D.C. Cir. 1990). The agency's affidavit regarding its search must be "reasonably detailed … setting forth the search terms and the type of search performed, and averring that all files likely to contain responsive materials were … searched." *Iturralde v. Comptroller of Currency*, 315 F.3d 311, 313-14 (D.C. Cir. 2003) (citation and internal quotation marks omitted).

Defendants' search was inadequate in three ways. First, defendants have not identified, either on their Vaughn indices or in their declarations, any extract identification or extract preparation records responsive to the first of plaintiffs' September 21, 2012, requests. Although the adequacy of an agency's search is "determined not by the fruits of the search, but by the appropriateness of [its] methods," *Iturralde*, 315 F.3d at 315, defendants provide no explanation of the search they undertook to locate the extract identification and preparation records. *See* Pineiro Decl. ¶ 31 (stating merely that, upon remand of plaintiffs' administrative appeal, ICE's FOIA office requested "additional searches"). Defendants' failure to provide any information regarding the searches performed precludes this Court from entering summary judgment in their favor with respect to the adequacy of their search.

Second, defendants' search of only the SLM depository for records responsive to plaintiffs' October 13 and 18, 2010, requests for a "complete set of documentation" on the EID and IIDS databases, respectively, is insufficient. Defendants state that "[t]he SLM repository is the authoritative place for technical documents associated with the EID and IIDS," Wilson Decl. at 5, and that "no other databases were required to be searched." *Id.* But elsewhere, defendants note that the metadata and schema records sought as part of the same requests were located in the EID and IIDS databases themselves. *See* Miller Decl. ¶ 7. Defendants thus have not

demonstrated that they searched all record systems that are "likely to produce responsive documents." *Oglesby*, 920 F.2d at 68.

Third, defendants failed to search any CBP records, even though plaintiffs requested CBP records. Peneiro Decl. Exs. 21, 23.

Accordingly, the Court should deny defendants' motion for summary judgment on the adequacy of their search and the Court should order defendants to conduct an adequate search for all responsive records.

CONCLUSION

For the foregoing reasons, this Court should grant plaintiffs' motion for summary judgment and order defendants to conduct an adequate search and deny the defendants' motion for summary judgment with respect to defendants' withholding of records pursuant to Exemption 7(E), their withholding of records on the basis that they lack the technology to produce the records, and the adequacy of their search.

Respectfully submitted,

s/ Jehan A. Patterson
Jehan A. Patterson
DC Bar No. 1012119
Scott L. Nelson
DC Bar No. 413548
PUBLIC CITIZEN LITIGATION GROUP
1600 20th Street NW
Washington, DC 20009
(202) 588-1000

Dated: November 13, 2014

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

SUSAN B. LONG and DAVID BURNHAM, Plaintiffs, v. IMMIGRATION AND CUSTOMS ENFORCEMENT and CUSTOMS AND BORDER PROTECTION, Defendants.	Civil Action No. 1:14-cv-0109 Judge John D. Bates

PLAINTIFFS' STATEMENT OF MATERIAL FACTS
AS TO WHICH THERE IS NO GENUINE ISSUE

1. On October 13, 2010, Plaintiffs Susan B. Long and David Burnham submitted a request to defendant Immigration and Customs Enforcement (ICE) for a "complete set of documentation on the Enforcement Integrated Database (EID)," including records identifying the database tables and fields within each table, records defining each code used in recording data in the EID, records of the EID's database schema (a class of records within a database system that sets forth how the database tables are interlinked), and records identifying the EID's software and the version number of that software. Long Decl. ¶ 4.

2. ICE responded by administratively closing the request on the basis that it had disclosed the database schema and codes in response to one of plaintiffs' prior FOIA requests. *Id.*

3. Plaintiffs appealed that closure and explained that this request was not duplicative of their prior request, and ICE remanded the request for additional searches. ICE did not provide any further responses. *Id.*

4. On October 18, 2010, plaintiffs submitted a FOIA request to ICE for a "complete set of documentation on the ICE Integrated Decision Support (IIDS) Database," including records identifying the database tables and fields of information stored in each table, records defining each code used in recording data in the IIDS, records of the IIDS database schema, and records identifying the IIDS's software and the version number of that software. *Id.* ¶ 5.

5. ICE responded by disclosing 97 pages with redactions pursuant to FOIA Exemption 7(E). *Id.*

6. Plaintiffs appealed, challenging the application of Exemption 7(E), the adequacy of ICE's search, and ICE's disclosure of only 97 pages of what appeared to be a larger document. On appeal, ICE affirmed the Exemption 7(E) withholdings and remanded the request for additional searches and re-processing of the larger document. ICE did not provide any further responses. *Id.*

7. On September 21, 2012, plaintiffs submitted two FOIA requests. In the first, they sought records "identifying any extracts and 'snapshots' prepared from the [EID] over the last 12 months" ("extract identification records"), as well as records identifying the frequency with which the extracts were prepared, who was responsible for preparing each extract, the recipients of those extracts, and the EID system time required to prepare each extract ("extract preparation records"). *Id.* ¶ 6.

8. ICE disclosed nine pages with redactions pursuant to FOIA Exemptions 6, 7(C), and 7(E). *Id.*

9. Plaintiffs appealed in part because the nine pages appeared to be summaries of various ICE records, and not the records themselves. They also appealed the Exemption 7(E) withholdings and ICE's failure to disclose any extract identification or extract preparation records. ICE remanded the request for additional searches and did not address plaintiffs' appeal of the Exemption 7(E) withholdings. ICE did not provide any further responses. *Id.*

10. Plaintiffs' second September 21, 2012, FOIA request was for the most current extract of data from the EID loaded into the IIDS as of the date the request would be processed. ICE never responded to this request. *Id.* ¶ 9.

11. On February 25, 2013, plaintiffs submitted a FOIA request to both ICE and defendant Customs and Border Protection (CBP) seeking the most current extract of data from the EID loaded into the CBP Data warehouse as of the date the request would be processed. *Id.* ¶ 10.

12. ICE responded that it had no responsive records, and plaintiffs did not appeal this denial. CBP, however, did not respond to plaintiffs' request. *Id.*

13. On February 26, 2013, plaintiffs submitted two FOIA requests. In the first request, plaintiffs sought from ICE the most current extract of data from the EID loaded into the ENFORCE Alien Removal Module (EARM) Datamart as of the date the request would be processed. ICE did not respond to this request. *Id.* ¶ 11.

14. In the second FOIA request, plaintiffs sought from both ICE and CBP the most current extract of data from the EID loaded into the EID Datamart. Neither ICE nor CBP responded to this request. *Id.*

15. Defendants have the technological capability to extract data from the EID and provide it in an electronic format to plaintiffs. Hasan Decl. ¶¶ 11-12.

16. ICE has the technological capability to produce extracts from the EID, IIDS, and associated databases, and provides such extracts on a recurring basis to other agencies and external entities, and has even disclosed such extracts to plaintiffs in response to prior FOIA requests. Patterson Decl. ¶ 2 & Ex. A at 20-22; Long Decl. ¶¶ 15-18 & Exs. I-L.

17. ICE has the technology and resources to redact data from extracts from the EID, IIDS, and associated databases. Long Decl. ¶¶ 17-18 & Exs. K-L; Hasan Decl. ¶¶ 14-15.

18. ICE furnishes EID data electronically to other agencies by "external interface connections in encrypted form" that require ICE to establish user accounts and execute a security agreement with the receiving agency. Patterson Decl. ¶ 2 & Ex. A at 22.

19. ICE also furnishes EID data electronically by uploading extract files to a secure file transfer protocol (FTP) server. *Id.* at 20-21.

20. For entities that lack the capability to exchange data through an electronic interface, ICE sends EID data in an encrypted email or on an encrypted DVD/CD that is delivered by a carrier service. *Id.* at 22.

21. The EID database has no publicly available electronic interface. *Id.* at 15.

22. Entities outside of the Department of Homeland Security (DHS) do not have direct access to the EID. *Id.* at 22.

23. ICE employs security measures to prevent unauthorized access to the EID and associated databases including, among other things, locking users out of sessions for inactivity, locking users out of their accounts after three failed attempts to access the system, implementing firewalls to protect network connections, regularly reviewing audit trails to detect unauthorized use or misuse, and requiring security training for authorized users. *Id.* at 28.

24. The disclosure of the requested records does not pose a credible threat to the security of the EID and associated databases and thus creates no viable risk of an external attack on the databases. Clark Decl. ¶¶ 12-17, 19-22.

25. None of the requested records reveals any techniques, procedures, or guidelines for law enforcement investigations or prosecutions. Long Decl. ¶¶ 14, 20.

26. Defendants did not search for the extract identification and extract preparation records responsive to the first of plaintiffs' September 21, 2012, FOIA request, Long Decl. ¶¶ 8, and their motion papers do not mention these records, demonstrate the adequacy of ICE's search for them, or justify their withholding.

27. Defendants' search of only the Systems Lifecycle Management (SLM) repository for records responsive to plaintiffs' October 13, 2010, FOIA request was inadequate because responsive records were also located in the EID itself. Wilson Decl. at 5; Miller Decl. ¶ 7.

28. Defendants' failure to search any CBP records responsive to plaintiffs' FOIA requests rendered defendants' search inadequate. Wilson Decl. at 7, 9.

Respectfully submitted,

s/ Jehan A. Patterson
Jehan A. Patterson
DC Bar No. 1012119
Scott L. Nelson
DC Bar No. 413548
PUBLIC CITIZEN LITIGATION GROUP
1600 20th Street NW
Washington, DC 20009
Tel: (202) 588-1000

Dated: November 13, 2014

Counsel for Plaintiffs