UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

MEMORANDUM OPINION AND ORDER

I. INTRODUCTION

This long-running case arises from Plaintiffs Susan B. Long and David Burnham's Freedom of Information Act ("FOIA") requests to Defendants Immigration and Customs Enforcement ("ICE") and Customs and Border Protection ("CBP"). As relevant here, Defendant ICE[1] withheld requested information from its Enforcement Integrated Database ("EID") and Integrated Decision Support Database ("IIDS") pursuant to FOIA Exemption 7(E). Following a third round of summary judgment briefing and an evidentiary hearing, the court ordered Defendant to conduct a segregability analysis as to the withheld information.

Defendant represents that it has since performed "[a] line-by-line review . . . to identify non-exempt information that could reasonably be segregated from the exempt portions" of the databases. Decl. of Tadgh Smith, ECF No. 101-3 [hereinafter Smith Decl.], ¶ 12. Having released that information, Defendant now moves for summary judgment. Defs.' Mot. for Summ. J.,

[1] Because all issues pertaining to the requests directed to Defendant CBP have been resolved, the court refers to ICE as the sole "Defendant" throughout this opinion and order.

ECF No. 101 [hereinafter Defs.' Mot.]. Plaintiffs oppose, pointing to several categories of information they contend should have been disclosed. *See* Pl.'s Mem. in Opp'n to Def.'s Mot., ECF No. 105 [hereinafter Pl.'s Opp'n].

For the following reasons, the court grants in part and denies in part Defendant's motion.[2] The court agrees that some of Defendant's continued withholdings are proper. But because Defendant failed to meet its burden to demonstrate that it properly withheld certain other information—now for a fourth time—it must disclose such non-exempt information in accordance with this Memorandum Opinion and Order.

II. BACKGROUND

The court has detailed the factual and procedural history of this case in its prior decisions. *See Long v. ICE* (*Long I*), 149 F. Supp. 3d 39, 43–47 (D.D.C. 2015); *Long v. ICE* (*Long II*), 279 F. Supp. 3d 226, 230–32 (D.D.C. 2017); *Long v. ICE* (*Long III*), 464 F. Supp. 3d 409, 412–16 (D.D.C. 2020). The court thus provides only the background necessary to resolve the remaining segregability dispute.

A. FOIA Requests I and II

Of Plaintiffs' seven FOIA requests, only requests I and II are unresolved. The first requested "a complete set of documentation on the [EID]." Defs.' Mot. For Summ. J., ECF No. 17 [hereinafter Defs.' First Mot.], Ex. 1, ECF No. 17-3. "The EID is the main repository of data for the enforcement of immigration law [by] ICE and CBP." *Long III*, 464 F. Supp. 3d at 412 (alteration in original) (quoting 5/18/2018 Hr'g Tr., ECF No. 62 [hereinafter Hr'g Tr.], at 16:1-2). It "captures and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations

[2] The court regrets the time it has taken to issue this decision and thanks the parties for their patience.

and operations conducted by [ICE], [CBP], and U.S. Citizenship and Immigration Services." *Long I*, 149 F. Supp. 3d at 44 (alterations in original) (quoting Decl. of Karolyn Miller, ECF No. 17-1 [hereinafter Miller Decl.], ¶ 12).

In their second FOIA request, Plaintiffs sought "a complete set of documentation on the [IIDS]." Defs.' First Mot., Ex. 8, ECF No. 17-3. The IIDS contains a subset of the information found in the EID, including "biographic information, information about encounters between agents/officers and subjects, and apprehension and detention information about all persons in EID." *Long I*, 149 F. Supp. 3d at 44–45 (quoting Miller Decl. ¶ 13). The IIDS is used primarily for reporting purposes. *Id.*; *Long III*, 464 F. Supp. 3d at 413.

For each database, the "complete set of documentation" Plaintiffs sought consisted of "records that (1) identified the names of EID and IIDS database tables and fields, (2) defined codes used to record data in those databases, (3) set forth the database schemas (that is, the way various database tables connect to each other), and (4) disclosed the particular software and version number used for the databases." *Long III*, 464 F. Supp. 3d at 414.

B. Defendant's Response and Procedural History

In response to these requests, Defendant released 97 pages from the IIDS, with redactions, and withheld all other responsive information pursuant to FOIA Exemption 7(E). *Id.* Exemption 7(E) permits an agency to withhold "records or information compiled for law enforcement purposes" if the requested information "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E). Unsatisfied with Defendant's disclosures, Plaintiffs filed suit.

On the parties' first cross-motions for summary judgment, the court agreed with Defendant that the information was "compiled for law enforcement purposes" and "qualif[ies], at least, as law enforcement guidelines, if not also law enforcement methods and techniques." *Long I*, 149 F. Supp. 3d at 48–50. At that time, however, Defendant had not provided enough evidence to substantiate that disclosure would risk circumvention of the law. While Defendant's claimed risk of "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," the court was "left unconvinced" on the record before it that disclosing the requested data would increase that risk. *Id.* at 51, 53. The court accordingly denied summary judgment. *Id.* at 53–54.

After allowing Defendant to supplement the record with additional evidence to support the asserted risk, the court again denied summary judgment. Despite the additional evidence, there remained "uncertainties on the record" as to the possibility of a cyber-attack that "create[d] triable issue[s] of fact as to the reasonableness of Defendant's expectation of risk of circumvention of the law." *Long II*, 279 F. Supp. 3d at 236. An evidentiary hearing followed. *See id.* at 245.

Following that hearing, the court concluded that disclosure of the requested data in its entirety could reasonably be expected to increase the risk of an effective cyber-attack. *See Long III*, 464 F. Supp. 3d at 419–23. But the court also concluded that Defendant likely had not released all segregable, non-exempt information. *Id.* at 424. Based on witness testimony, it seemed that "only metadata that 'describes the organization of [ICE's] data and the structure of its databases[]' presents any risk." *Long III*, 464 F. Supp. 3d at 425 (quoting Hr'g Tr. at 62:21-22). That kind of data could provide a "thieves' map" that "would assist a hacker in launching a more targeted and effective attack that is less likely to be detected by the agency." *Id.* at 422. While "the database schemas (which, by definition, describe the structure of ICE's databases) present such a material

risk," the "other categories of information requested by Plaintiffs—field and table names, codes, code translations, and code lookup tables—do not appear to uniformly pose such a risk." *Id.* at 425. The court ordered Defendant to conduct a segregability analysis as to the latter categories of data. *Id.* at 426–27.

Defendant represents it has since performed a "line-by-line" segregrability analysis, disclosing some data to Plaintiffs and withholding other records pursuant to Exemptions 6, 7(C), and 7(E). Smith Decl. ¶¶ 4, 12. Only the claimed exemptions under 7(E) are disputed. *Id.* ¶ 4.

III. LEGAL STANDARD

A court "shall 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). A "genuine" dispute is one in which a rational trier of fact could find for the nonmoving party based on the record before it. *Scott v. Harris*, 550 U.S. 372, 380 (2007) (quoting *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586–87 (1986)).

In a FOIA case, the agency bears the burden of demonstrating that it properly withheld information from disclosure. *Campaign for Resp. Transplantation v. FDA*, 511 F.3d 187, 190 (D.C. Cir. 2007) (citing *U.S. Dep't of Just. v. Reps. Comm. for Freedom of the Press*, 489 U.S. 749, 755 (1989)). Establishing that Exemption 7(E) applies is a "relatively low bar." *Blackwell v. FBI*, 646 F.3d 37, 42 (D.C. Cir. 2011). The agency need not show a "certain risk of circumvention." *Id.* (quoting *Mayer Brown LLP v. IRS*, 562 F.3d 1190, 1193 (D.C. Cir. 2009)). It need only "demonstrate logically how the release of the requested information might create a risk of circumvention of the law." *Id.* (quoting *Mayer Brown*, 562 F.3d at 1194). While this standard is "deferential," the court's review is not "vacuous." *Campbell v. U.S. Dep't of Just.*, 164 F.3d 20, 32 (D.C. Cir. 1998) (internal quotation marks and citations omitted). The agency must

provide sufficient facts to support the asserted risk. *New Orleans Workers' Ctr. for Racial Just. v. ICE*, 373 F. Supp. 3d 16, 66 (D.D.C. 2019).

Even if the agency demonstrates that an exemption applies, it must still "disclose 'any reasonably segregable portion of a record' after removing the exempt material and must note the 'amount of information deleted, and the exemption under which the deletion is made.'" *Bartko v. U.S. Dep't of Just.*, 898 F.3d 51, 62 (D.C. Cir. 2018) (cleaned up) (quoting 5 U.S.C. § 552(b)). The agency is "entitled to a presumption that [it] complied with the obligation to disclose reasonably segregable material." *Sussman v. U.S. Marshals Serv.*, 494 F.3d 1106, 1117 (D.C. Cir. 2007). But the agency still "must provide a 'detailed justification' and not just make 'conclusory statements' to support its segregability determination." *Levinthal v. FEC*, 219 F. Supp. 3d 1, 9 (D.D.C. 2016) (quoting *Mead Data Cent., Inc. v. U.S. Dep't of the Air Force*, 566 F.2d 242, 260 (D.C. Cir. 1977)). And the requester may overcome the presumption with contrary evidence, at which point "the burden lies with the government to demonstrate that no segregable, nonexempt portions were withheld." *Sussman*, 494 F.3d at 1117.

IV. DISCUSSION

After performing its segregability analysis, Defendant withheld four categories of information under Exemption 7(E): information that would "(A) link information between [ICE] database elements, (B) link information to other law enforcement databases, (C) reference sensitive law enforcement programs, and/or (D) identify current and active sensitive elements of the [EID or IIDS] database[s]." Smith Decl. ¶ 9.

Before addressing these categories of withholdings, the court briefly addresses Plaintiffs' argument that Defendant has waived all these justifications for withholding information except for the first. Relying on *Maydak v. United States Department of Justice*, 218 F.3d 760 (D.C. Cir.

2000), Plaintiffs reason that Defendant was required to raise these justifications during earlier summary judgment briefing or at the evidentiary hearing to preserve them. Pl.'s Opp'n at 21–23. But *Maydak* is distinguishable. There, the D.C. Circuit held that the agency did not adequately assert several FOIA exemptions because the agency cited varying exemptions at different stages of the litigation and because it "made no attempt to substantiate" the claimed exemptions. *Maydak*, 218 F.3d at 765. By contrast, here, Defendant has maintained that Exemption 7(E) permits it to withhold the redacted information from the outset. Moreover, Defendant has substantiated its Exemption 7(E) claims at least in part by citing the rationales it now relies on. Defendant has previously stated that "systems operated by other federal agencies . . . are interconnected to ICE's EID and IIDS databases" and that, if it were to disclose the requested data, "an attacker may mount attacks on other interconnected systems." Defs.' Suppl. Br. in Supp. of Defs.' First Mot., ECF No. 35, at 11–12 (citing Decl. of J. Thomas Foster, ECF No. 32-3, ¶¶ 10, 20, 21). Defendant also has argued that disclosing the withheld data risks the "potential manipulation of information related to ongoing investigations." *Id.* at 5. Defendant therefore has not waived its asserted justifications for withholding information.

A. Links Between ICE Database Elements

Defendant first withheld "the attribute names, definitions, and data type of Foreign and Primary keys in the EID Data Dictionary," as well as the same information in the IIDS Data Dictionary. Smith Decl. ¶ 9(A). The "Data Dictionary" lists the names of the tables and fields contained in each database. *Long III*, 464 F. Supp. 3d at 418. The primary and foreign keys are the fields that reveal how the database's tables are connected to one another. A primary key is a unique identifier for a particular field in a data table. Smith Decl. ¶ 9(A). And a foreign key is a field that incorporates the primary key into another data table by cross-reference. *Id.* For example,

an EID table called "Attorney" contains information about attorneys involved in ongoing cases, such as their names and law firms. Pl.'s Opp'n at 6 (citing Pl.'s Opp'n, Ex. PPP, ECF No. 105-2 [hereinafter Ex. PPP]). Each attorney is identified by a unique "Attorney ID" code. *Id.* In the "Attorney" table, "Attorney ID" is a primary key. *Id.* A different EID table, the "Case" table, lists the attorney associated with each case by their "Attorney ID" code. *Id.* at 5–6. To find out who the attorney is, one would then need to go to the "Attorney" table and find the corresponding "Attorney ID." *Id.* at 6. So, in the "Case" table, the "Attorney ID" functions as a "foreign key[] that point[s] to data in [an]other table[]." *Id.* By following the foreign key (in the cross-referencing table) to the primary key (in its original table), one can discern how different elements of ICE databases are linked. Smith Decl. ¶ 9(A).

For that reason, Defendant withheld information that reveals primary and foreign keys. As Defendant sees it, "[k]nowing the design of the system (having awareness how elements of the database relate or link to each other) increases the likelihood that agency systems may be compromised since it provides adversaries knowledge of the most vulnerable entry points and avenues of success for an attack." *Id.* This knowledge may also allow for attacks that are less easily detected, as a hacker could "pass off the attack more convincingly" as "authentic" activity. *Id.* A hacker could then modify or delete sensitive law enforcement data. *Id.*

Plaintiffs do not dispute that the names of the fields constituting primary and foreign keys can be withheld. Pl.'s Opp'n at 6. But they argue that the court's opinion in *Long III* allows for no more. *See id.* at 6–9. So, Plaintiffs reason, Defendant acted contrary to the court's order by continuing to withhold three kinds of information that purportedly demonstrate links between ICE database elements: (1) the definitions and data type of primary and foreign keys; (2) the plain-English translations of primary and foreign keys in the EID Data Dictionary; and (3) the names,

definitions, and data type of codes that are translated in separate code lookup tables. *Id.* at 7–8. Plaintiffs also point to a small group of miscellaneous withholdings that they contend are entirely unrelated to primary and foreign keys. *See id.* at 16–20.

1. Definitions and Data Types of Primary and Foreign Keys

As previously mentioned, Defendant redacted the definitions and data type of primary and foreign keys in each data dictionary. Smith Decl. ¶ 9(A). The definitions are "the English-language descriptions of the information" contained in each field. Pl.'s Opp'n at 8. And the data type shows whether the field's code is expressed in numbers, letters, or another combination of characters. *See id.* Plaintiffs contend that, under *Long III*, Defendant could not withhold either. *Id*.

Plaintiffs read *Long III* too narrowly. The court ordered Defendant to determine "whether linkage fields *and other sensitive data* can be redacted." 464 F. Supp. 3d at 427 (emphasis added). Instead of speaking in absolutes, the court recognized that "the codes and code translations within *certain* code lookup tables could be released without creating an unacceptable threat to the security of the EID and IIDS databases," and that such disclosures "do not appear to *uniformly* pose [] a risk." *Id.* at 424–25 (emphases added). In short, while recognizing that some information other than field names could be disclosed, the court expressly gave Defendant leeway to redact such information where it poses a security risk.

Plaintiffs also contend that Defendant's choice to redact more than just linkage field names conflicts with the evidentiary-hearing testimony of Tadgh Smith, an ICE official familiar with the agency's databases.[3] Pl.'s Opp'n at 8–9. To be sure, Smith acknowledged that, in some instances, disclosing plain-English descriptions of fields would not pose a threat. *See, e.g.*, Hr'g Tr. at 62:3-

[3] Smith's full title is Deputy Assistant Director of the Law Enforcement Systems and Analysis Division, within the Enforcement and Removal Operations, at ICE. Smith Decl. ¶ 1.

9. But Smith consistently maintained that some information is more sensitive than others, even when presented in plain English. *See, e.g., id.* at 56:7-11, 63:9-12. Smith's testimony is thus consistent with Defendant's choice to sometimes withhold information beyond just the names of linkage fields.

Plaintiffs do not otherwise offer evidence to refute Defendant's contention that disclosing the definitions and data type of primary and foreign keys would risk circumvention of the law. Meanwhile, Defendant avers that the "few English-language descriptions that have been withheld describe and comprise the Primary and Foreign Keys themselves—for example, where the information within these fields is being pulled from or is being pulled by other database elements." Second Decl. of Tadgh Smith, ECF No. 110-1 [hereinafter Second Smith Decl.], ¶ 7. Disclosing this information would therefore "reveal the database structure and a potential wrong doer would be able to identify how the information is linked to other database elements," which renders the database more vulnerable to attack. *Id.* This is precisely the risk the court has already recognized justifies withholding under Exemption 7(E). *See Long III*, 464 F. Supp. 3d at 419–23; *see also, e.g.*, *Tracy v. U.S. Dep't of Just.*, 191 F. Supp. 3d 83, 96–97 (D.D.C. 2016). Seeing no genuine dispute of material fact on this point, the court concludes that Defendant properly withheld the definitions and data type of primary and foreign keys.[4]

[4] Plaintiffs identified two small sets of redactions that Smith did not explain in his initial Declaration. Pl.'s Opp'n, Fifth Decl. of Susan Long, ECF No. 105-1 [hereinafter Long Decl.], ¶ 51. In his supplemental declaration, Smith clarified that the withholdings fell into the category of information redacted because it would reveal links between ICE database elements. Second Smith Decl. ¶ 25. One of the two sets of redactions is comprised of "field names, definitions, and data types" in the IIDS Data Dictionary. Long Decl. ¶ 53. Plaintiffs acknowledge that this set "may reflect redaction of fields representing primary or foreign keys." *Id.* Plaintiffs' only objection is that, even if it does, Defendant can withhold only the names of the linkage fields, not their plain-English descriptions or data types. *Id.* As discussed above, however, *Long III* does not limit Defendant's ability to withhold this information. Defendant thus properly redacted it.

2. Plain-English Translations in the EID Data Dictionary

Plaintiffs next take issue with Defendant's redacting the plain-English translations of primary and foreign keys in the EID Data Dictionary. Pl.'s Opp'n at 9. To continue with the earlier example, "Attorney ID" is the plain-English translation of the field "CSE_Aty_ID." *Id.* at 10. These plain-English translations "make the data more accessible to the requester by describing it for what it is rather than the abbreviation of the field." Hr'g Tr. at 60:5–61:4. Without the translations, the data would "appear as largely strings of unintelligible letters and numbers." Pl.'s Opp'n, Fifth Decl. of Susan Long, ECF No. 105-1 [hereinafter Long Decl.], ¶ 22.

Defendant withheld the translations as "part of the essential 'linkage' portions of the database that are protected." Second Smith Decl. ¶ 8. Disclosing this information, Defendant maintains, "would essentially be providing a potential wrongdoer the information necessary to determine what fields are linked throughout the databases." *Id.* Defendant, however, provides nothing more than this general assertion to justify withholding the translations. Unlike its reasoning for withholding definitions and data types, which identifies the risk attendant to disclosing that specific information, Defendant's explanation here does not provide sufficient facts to "demonstrate logically" how disclosure would facilitate a cyberattack. *Blackwell*, 646 F.3d at 42; *see also Am. Immigr. Council v. ICE*, 464 F. Supp. 3d 228, 243–44 (D.D.C. 2020).

Additionally, Defendant's vague explanation is in tension with Smith's testimony at the evidentiary hearing. There, Smith stated that while disclosing field names may create a security risk, Defendant regularly discloses plain-English translations "[a]s an attempt to mitigate that threat." Hr'g Tr. at 61:17–62:9. Smith now submits that his "prior testimony about plain-English versions as a mitigation strategy does not apply to Primary and Foreign keys." Second Smith Decl. ¶ 8. But this conclusory statement is insufficient to explain why. *See Lykins v. U.S. Dep't of Just.*,

725 F.2d 1455, 1463 (D.C. Cir. 1984) ("[T]he government may not justify withholding information in FOIA cases on the basis of sweeping or conclusory statements concerning the applicability of FOIA exemptions.").

Defendant's explanation also appears to be belied by contemporaneous disclosures. *See Long III*, 464 F. Supp. 3d at 425. In response to a separate FOIA request, Defendant released a spreadsheet to Plaintiffs in March 2023. Long Decl. ¶ 25. The spreadsheet contains plain-English translations of field names that appear to be redacted as primary and foreign keys in the EID Data Dictionary at issue in this litigation. *Compare id.* ¶ 25, *and* Pl.'s Opp'n, Ex. QQQ, ECF No. 105-3 (containing plain-English translations of headers such as Detainer ID, Subject ID, and Government Employee ID, among others), *with* Def.'s Mot., Ex. 5 (submitted via CD) [hereinafter Ex. 5] (appearing to redact those plain-English translations for the relevant codes). Citing the sensitivity of this information, Defendant neither confirmed nor denied whether these plain-English translations in the more recent disclosure are the same as the ones redacted in the EID Data Dictionary. Second Smith Decl. ¶ 8. The court acknowledges that Defendant may not be able to disclose certain details about withheld information in public filings. *See Lykins*, 725 F.2d at 1463–64. Yet where, as here, Plaintiffs have pointed to prior conflicting testimony and contemporaneous disclosures that dispute the sensitivity of this information, Defendant must provide more. *Cf. Gov't Accountability Project v. CIA*, 633 F. Supp. 3d 171, 175 (D.D.C. 2022) ("[E]ven where an agency declines to confirm or deny that it maintains any responsive records, it still bears the burden of justifying its decision."). It has not done so. Therefore, Defendant has not carried its burden.[5]

[5] Throughout its reply brief, Defendant repeatedly cites a footnote from *Long III* that it argues renders Plaintiffs' references to prior disclosures irrelevant. *See* Def.'s Reply in Further Supp. of Def.'s Mot., ECF No. 110 [hereinafter Def.'s Reply], at 5 n.2, 10, 12, 13. The footnote, which acknowledges that some of Defendant's prior disclosures

It bears emphasizing that Defendant had the opportunity to submit responsive evidence with its reply brief. Yet, for this category of information and others, Defendant either failed to do so or stated that it could neither confirm nor deny details about the withholdings. The former is clearly insufficient, and the court does not find the latter explanation compelling. Defendant could have submitted for *in camera* review any evidence it viewed as too sensitive to be disclosed in public filings but chose not to do so. *See Roth v. U.S. Dep't of Just.*, 642 F.3d 1161, 1185 (D.C. Cir. 2011) (stating that an agency may supplement public explanations for withholdings with *in camera* submissions "when extensive public justification would threaten to reveal the very information for which a FOIA exemption is claimed" (internal quotation marks and citation omitted)). Defendant therefore has not met its burden to demonstrate that it properly redacted information withheld as revealing plain-English translations of primary and foreign keys and must disclose this information to Plaintiffs.

3. Field Names Representing Codes Translated in Separate Code Tables

Defendant also withheld "field names, definitions, and logical data types within data tables in the EID and IIDS Data Dictionaries where the field names are codes that are defined in separate code lookup tables." Pl.'s Opp'n at 12 (citing Long Decl. ¶ 11). Defendant states that this information can "reveal linkages or provide insight into the EID and IIDS structure" because the codes are foreign keys in their respective data tables. Second Smith Decl. ¶ 9. The codes direct users to code lookup tables, where the codes are translated into plain English. Pl.'s Opp'n at 11.

---

were inadvertent and that the databases have since been updated, states that "these particular disclosures do not have any bearing on the reasonableness of ICE's withholdings under Exemption 7(E) or the adequacy of the agency's segregability analysis." *Long III*, 464 F. Supp. 3d at 424 n.16. For starters, some of the exhibits Defendant now characterizes as inadvertently disclosed were described otherwise at the evidentiary hearing. *Compare* Def.'s Reply at 10 (describing Exhibit DDD as a mistakenly produced document), *with* Hr'g Tr. at 78:15-18, 79:5-14 (stating the opposite). Additionally, even where the prior disclosures on which Plaintiffs rely were mistaken, Defendant overreads this footnote. The court maintains that these prior disclosures are not dispositive. But Plaintiffs have used them as evidence that Defendant has improperly withheld certain information, and Defendant may not summarily dismiss these contentions as based on older versions of the databases to avoid its burden to overcome them.

Here again, Defendant's wholesale withholding of this information contradicts Smith's testimony at the evidentiary hearing. For example, Defendant redacted the name, description, and data type for the "Detention Facility Type Code" in the EID Data Dictionary. Pl.'s Opp'n at 13; *see also* Ex. 5. Yet, at the evidentiary hearing, Smith testified that this field is not a linkage field. Hr'g Tr. at 97:21–98:1. Smith testified similarly regarding other examples of codes defined in the code lookup tables. *See id.* at 64:2-20. Defendant does not attempt to explain these inconsistencies.

The notion that these fields are not linkage fields is bolstered by what Plaintiffs identify as an inconsistency in how Defendant redacted them. For a true primary or foreign key, Defendant withheld the code as both a primary key in the original table and as a foreign key in the table that cross-references it. Pl.'s Opp'n at 14–15. To return to the running example, Defendant withholds the code for the "Attorney ID" field in both the "Attorney" table (where it is a primary key) and the "Case" table (where it is a foreign key). *Id.* Yet for the codes at issue here, Defendant redacted them in the data tables (where it claims they are foreign keys), but not in the code lookup tables (where they would ostensibly be primary keys). *Id.* at 15; *see also* Def.'s Mot., Ex. 1 (submitted via CD). Once again, Defendant does not attempt to explain this discrepancy.

Defendant thus has not adequately responded to Plaintiffs' evidence that it improperly withheld codes that are separately defined in code lookup tables. In his supplemental declaration, Smith states that revealing these field names "would link this information to other database elements in the code lookup tables *and elsewhere*." Second Smith Decl. ¶ 9 (emphasis added). But this "vague" description of the purported linkages to other data tables "provides the Court with no means by which it can determine whether disclosure could result in evasion of the law."

New Orleans Workers' Ctr., 373 F. Supp. 3d at 66–67 (cleaned up). Defendant has not carried its burden, and it must disclose this category of information.

4. Miscellaneous Withholdings

Although they do not fall neatly into one of the groups of redactions already discussed, Plaintiffs identify several other redactions Defendant claims would have revealed linkages between ICE database elements that Plaintiffs contend are unrelated to linkage fields. For the majority of them, Plaintiffs have put forward contrary evidence that Defendant has failed to overcome. Defendant must therefore disclose the withheld information.

Table Names and Descriptions. Recall that primary and foreign keys are field names. *See supra* Section IV.A. Yet, on the basis that they reveal primary and foreign keys, Defendant has redacted portions of plain-English translations of *table* names in both the EID Data Dictionary and IIDS Data Dictionary, and of table descriptions in the latter. *See* Long Decl. ¶¶ 6–7; Pl.'s Opp'n at 18. Defendant does not provide an explanation to bridge this gap.

Some examples of the apparent redactions cast further doubt on their propriety. Defendant appears to have redacted the prefix "EID" from at least one table name in the IIDS Data Dictionary. *Id.* A prefix revealing that the information came from the EID—of which it is publicly known that the entire IIDS is a subset—does not seem to reveal secure linkage information. Defendant thus has not shown that it was entitled to withhold portions of table names and descriptions under Exemption 7(E).

Field Names. The court is not, however, in a position to question Defendant's withholding of various field names in the EID Dictionary that Plaintiffs contend are not linkage fields. *See* Long Decl. ¶ 6. Defendant states it redacted these field names because they reveal information about "internal and external database codes, systems, and identifiers." Second Smith Decl. ¶¶ 10–

11. Plaintiffs' conclusory claim to the contrary is not enough for this court to doubt Defendant's representation. *See SafeCard Servs., Inc. v. SEC*, 926 F.2d 1197, 1200 (D.C. Cir. 1991).

Field Descriptions. In some cases, Defendant did not redact the name of a field as a primary or foreign key, yet still redacted portions of the description of the field as describing a primary or foreign key. Pl.'s Opp'n at 18–19. Without further explanation from Defendant, the court agrees with Plaintiffs that, "[i]f the name of such a field is not claimed as a primary or foreign key name, its description cannot be withheld on the basis that it describes the attributes of a primary or foreign key." *Id.* at 18.[6]

Code Lookup Tables "Create By" Column. Plaintiffs lastly point to "partial or complete redaction[s] of the code description and code 'create by' columns for two codes" in the EID code lookup tables. Pl.'s Opp'n at 20. Plaintiffs argue that this information—and, for that matter, any information contained in the EID code lookup tables—does not reveal linkages between EID data tables. *Id.* at 19–20. Defendant responds that any information redacted from the EID code lookup tables reveals linkages. Second Smith Decl. ¶ 12.

Plaintiffs' own example bears out Defendant's position. By comparing the redactions to a disclosure made pursuant to a separate FOIA request, Plaintiffs determined that Defendant appears to have redacted the acronym "EARM" from several entries in the "create by" column for one of the EID code lookup tables. Long Decl. ¶ 39; *see* Pl.'s Opp'n, Ex. SSS, ECF No. 105-5. EARM, the Enforcement and Removal Module, is a module of the EID. Long Decl. ¶¶ 39, 47. The information in this column "signifies that the relevant code was created through the EARM." *Id.*

[6] The second set of initially unexplained redactions are omissions from field descriptions in the EID Data Dictionary. Long Decl. ¶ 52. These redactions are also often from descriptions of fields for which the field names were not redacted as revealing primary or foreign keys. *See* Ex. 5.

¶ 39. This information could accordingly "reveal . . . how data is linked to internal and external database elements." Second Smith Decl. ¶ 13. Defendant therefore properly redacted it.

B. Links to Other Law Enforcement Databases

The second category of information Defendant withheld is information that reveals linkages to other law enforcement databases. Smith Decl. ¶ 9(B). This information shows how other law enforcement databases use, or are used by, the EID and IIDS. *Id.* So, Defendant withheld it on the basis that potential hackers could exploit the information to assess vulnerabilities and engineer attacks not only on Defendant's databases, but also systems belonging to other law enforcement agencies like CBP, the FBI, or the Department of State. *Id.* The hacker could then modify or delete data across multiple agencies' systems, allowing dangerous individuals to evade custody. *See id.*

Defendant may withhold information that poses such a risk. *See, e.g.*, *Smith v. Sessions*, 247 F. Supp. 3d 19, 27–28 (D.D.C. 2017). But it has not shown that all the information it withheld pursuant to this rationale does so.

For all currently active law enforcement databases, Defendant may withhold this information. *See New Orleans' Workers Ctr.*, 373 F. Supp. 3d at 69 (noting that whether "any such operation remains in effect" is relevant to the analysis). For example, Defendant withheld what Plaintiffs posit are references to the IDENT database, which several law enforcement agencies use for fingerprints and other biometric data. Pl.'s Opp'n at 24 (citing Long Decl. ¶ 37). Defendant also withheld supposed references to the SEACATS database, which "is the information system of record for the full lifecycle of all enforcement incidents related to CBP and U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) operations." Long Decl. ¶¶ 37, 47. It "tracks the physical inventory and records disposition of all

seized assets, as well as the administrative and criminal cases associated with those seizures, and functions as the case management system capturing the relevant information and adjudication of the legal outcomes of all fines, penalties, and liquidated damages." *Id.* ¶ 47. Defendant did the same with respect to assumed references to the TECS database, which "serves as a data repository to support law enforcement 'lookouts,' border screening, and reporting for CBP's primary and secondary inspection processes." *Id.* ¶¶ 37, 47. References to each of these databases show how "information is pulled from an external database and analyzed alongside other information" in Defendant's databases. Smith Second Decl. ¶ 13. Such information could "logically," *Blackwell*, 646 F.3d at 42, reveal "how ICE's databases are linked to other systems and databases" and provide information as to their structures, rendering them more vulnerable to attack, Second Smith Decl. ¶ 13; *see Skinner v. U.S. Dep't of Just.*, 893 F. Supp. 2d 109, 114 (D.D.C. 2012) (citing cases allowing agencies to redact information from the TECS database to prevent unauthorized access).

Plaintiffs' primary objection to Defendant withholding this information is that it is already public. Plaintiffs note that Defendant is required to disclose use of these databases through statutorily required Privacy Impact Assessments and Systems of Records Notices, so this information "cannot be claimed as exempt on the basis that it would 'reveal' something that is not already widely known." Long Decl. ¶¶ 29–32, 37. Plaintiffs also point to the nine-page document Defendant was required to disclose earlier in this litigation, which it contends "contains extensive discussions of the relationships among various ICE databases . . . as well as databases of other agencies." Pl.'s Opp'n at 28 (first citing Pl.'s Opp'n, Ex. RRR, ECF No. 105-4; then citing Long Decl. ¶ 32).

As an initial matter, Defendant responds that some of the withheld information pertains to databases that are not publicly known. Second Smith Decl. ¶ 15. Defendant may continue to

withhold such information. For those that are publicly known, Defendant does not claim to have withheld this information merely because it reveals that Defendant uses them. Instead, Defendant withheld this information because it reveals *how* Defendant uses the databases and, in turn, how they and Defendant's databases are interconnected. Second Smith Decl. ¶¶ 13, 24. This information is not publicly known. And the nine-page document does not reveal "precisely how ICE connects those databases within [its] own databases." *Id.* ¶ 23. Disclosing this information would therefore reveal non-public information that could risk circumvention of the law. *See Am. Immigr. Laws. Ass'n v. U.S. Dep't of Homeland Sec.*, 485 F. Supp. 3d 100, 112 (D.D.C. 2020) ("[T]he presence of unredacted, publicly available information . . . does not overcome [the agency's] decision to withhold information in these documents under Exemption 7(E). That is because *how* [the agency] employs public information may not be known and can itself disclose law enforcement techniques and procedures."); *Shapiro v. U.S. Dep't of Just.*, 893 F.3d 796, 800 (D.C. Cir. 2018) (upholding the agency's withholding under Exemption 7(E) because, "[t]hough the capabilities of [the database] might be known to the public, the [agency's] methods of managing the database are generally not known"). Defendant properly withheld this information.

Plaintiffs, however, have provided evidence that Defendant wrongly withheld some of the redacted information as revealing connections to other law enforcement databases. For example, Plaintiffs point to (1) redactions of the prefix "EID" from some field names in the IIDS Data Dictionary, which refers to an *internal* ICE database, Long Decl. ¶¶ 35–36; (2) redactions that seem to refer to databases that are no longer in use, such as the DACS, which has since been migrated to the EID, *id.* ¶¶ 38, 47; and (3) redactions that appear to refer to acronyms that do not stand for databases at all, such as ATD, which stands for "Alternatives to Detention," *id.* ¶ 37; Pl.'s Opp'n at 25. As before, Defendant declined to confirm or deny whether Plaintiffs correctly

identified the withheld information. Second Smith Decl. ¶ 13. But if Plaintiffs are correct, not all information withheld as revealing linkages to other law enforcement databases actually does so. Because Defendant has not met its burden to overcome this contrary evidence, it must disclose all information withheld on this basis that does not reveal details about currently active law enforcement databases.

C. Joint Law Enforcement Operations

Defendant also withheld information about "sensitive law enforcement programs," including joint operations with other law enforcement entities. Smith Decl. ¶ 9(C). Defendant avers that these programs are not known to the public and that, if they became known, it would "jeopardize the mission, the officers involved, and the subjects under investigation." *Id.* Knowledge of these programs "would allow numerous opportunities to evade law enforcement" or "to intimidate, threaten, harm, or kill members of the public and protected immigrants, ICE officers and other law enforcement agency personnel." *Id.*

Whether Defendant was justified in withholding this information is similar to whether Defendant was justified in withholding information that it claimed reveals linkages to other law enforcement databases. *See supra* Section IV.B. Where Defendant withheld information about ongoing law enforcement operations, it may continue to withhold that information. *See New Orleans' Workers Ctr.*, 373 F. Supp. 3d at 69. Defendant again appeared to redact references to the IDENT database on this basis. Long Decl. ¶ 43. Defendant also redacted a portion of the IIDS Data Dictionary's description of the 287(g) program, which is a joint immigration law enforcement program between state and federal officers. *Id.* ¶ 45. The description reads in part: "The data for this table is received from a [REDACTED] representative." *Id.* While Plaintiffs are correct that the 287(g) program itself is public knowledge, they do not contend that the identities of the

representatives from which Defendant receives the pertinent information are public. It is thus reasonable to conclude that "release of this information would reveal law enforcement methods for investigating or prosecuting a crime." Second Smith Decl. ¶ 14.

But Defendant also withheld information under this rationale that does not seem to reveal sensitive law enforcement operations. For example, Defendant appears to have redacted the prefix "INS" from a table name in the IIDS Data Dictionary. Long Decl. ¶ 44. INS stands for Immigration and Naturalization Service, ICE's now-defunct predecessor agency. *Id.* References to an agency that no longer exists do not appear to reveal sensitive law enforcement operations.[7] Nor do the redacted parts of the description for a table containing information about proceedings before immigration judges or the Board of Immigration Appeals. *See* Long Decl. ¶ 45. These adjudicatory proceedings are not "joint-agency law enforcement programs." Smith Decl. ¶ 9(C). Defendant does not argue otherwise.[8]

Once again, Defendant has failed to adequately respond to Plaintiffs' evidence suggesting that some information redacted pursuant to this rationale was improperly withheld. Defendant must disclose all data withheld on this basis that is not related to ongoing law enforcement operations.

[7] Defendant acknowledges that its databases contain information about law enforcement operations that is "many years old." Second Smith Decl. ¶ 15. But Defendant continues that "some operational aspects of the data and information contained within the documents may still be current, and some of the information ICE is mandated to protect." *Id.* To the extent that any seemingly outdated information falls into this category, Defendant need not disclose it.

[8] Defendant notes that, to attempt to discern the contents of these redactions, Plaintiffs "checked [these redactions] against the partial IIDS schema in Exhibit DDD." Pl.'s Opp'n at 29. Defendant argues that, because the court stated in *Long III* that "ICE need not conduct an additional segregability analysis as to the database schemas," "Plaintiffs' reliance on Exhibit DDD in this context impermissibly seeks to expand this Court's rulings on what ICE needed to conduct a segregability analysis." Def.'s Reply at 11–12. Plaintiffs, however, do not seek any additional disclosures from the database schemas. Instead, using old versions of the schemas as a reference, Plaintiffs attempted to determine whether Defendant should have disclosed additional information in the data tables. That is not at odds with the court's prior order.

D. Current and Sensitive Operations

Defendant lastly withheld information that reveals "information pertaining to ongoing operations and other actively used elements of law enforcement that are not known to the public." Smith Decl. ¶ 9(D). This includes "the various definitions associated with codes assigned to individuals proceeding through the immigration process, the names and elements associated with law enforcement operations, and codes pertaining to weapons and assets recovered during law enforcement operations." *Id.* Defendant maintains that revealing this data would enable potential hackers to access, modify, or delete real-time data pertaining to ongoing investigations, which would prevent Defendant from fulfilling its duties and threaten the safety of protected subjects, law enforcement officers, and the public. *See id.*

Plaintiffs acknowledge that "some of the information withheld . . . on this basis . . . may relate in some way to such operational concerns." Pl.'s Opp'n at 32. By this point, the reason why is familiar. Defendant redacted references to several active law enforcement databases on this basis, such as references to IDENT, SEACATS, and TECS. Long Decl. ¶ 47. Defendant properly withheld this information. *See supra* Section IV.B.

But, once again, Defendant's redactions seem to exceed its stated justification. Pursuant to this justification, Defendant again appeared to redact the prefix "EID" from some field names in the IIDS code lookup tables, as well as references to former databases like the DACS.[9] Long Decl. ¶ 47. Defendant also redacted field names and descriptions in the "Field Office Director History" table in the EID Data Dictionary, which merely provides "the periods of time when

[9] Plaintiffs also point to Defendant's likely redactions of references to the LYNX database, which it describes as "very old." Long Decl. ¶ 47. The court declines to equate "old" with "defunct." As Defendant states, although some of the information regarding its law enforcement efforts may be old, some operational aspects may still be current. Second Smith Decl. ¶ 15. Defendant therefore properly withheld references to the LYNX database, as well as to any other database which, while perhaps older, is still used as part of ongoing law enforcement operations. *See supra* Section IV.B–C.

former field office directors and director designees held office." Long Decl. ¶ 48. Or, in the IIDS code lookup tables, Defendant seems to have redacted the heading and contents of a column entitled "INTERNET_INFORMATION_SERVER_CD," which identifies the URL addresses of various federal courts. *Id.* ¶ 47. Defendant does not explain how disclosing any of this information would reveal ongoing, sensitive law enforcement operations.

Defendant thus has not shown that disclosing all the information redacted pursuant to this rationale would risk circumvention of the law. Defendant must disclose all information in this category that does not relate to ongoing, sensitive law enforcement operations.

V. CONCLUSION AND ORDER

For the foregoing reasons, the court grants in part and denies in part Defendant's Motion for Summary Judgment, ECF No. 101. The court denies as moot Plaintiffs' Motion for Leave to File a Surreply, ECF No. 111. The court orders Defendant to disclose the following information to Plaintiffs:

1. For information withheld as revealing linkages between ICE database elements, all plain-English translations of primary and foreign keys; all field names constituting codes that are separately defined in code lookup tables; all redactions from table names and descriptions; and all redactions from descriptions of fields for which the field name was not redacted as revealing a primary or foreign key.
2. For information withheld as revealing linkages to other law enforcement databases, all information unrelated to currently active law enforcement databases.
3. For information withheld as revealing sensitive law enforcement programs or joint law enforcement operations, all information unrelated to ongoing programs or operations.

4. For information withheld as revealing current and sensitive law enforcement operations, all information unrelated to ongoing operations.

The parties shall submit a Joint Status Report apprising the court of Defendant's progress on this production no later than January 16, 2026. The court will enter a final order once the parties confirm the production is complete.

Dated: December 2, 2025

Amit P. Mehta
United States District Judge