UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

RONALD L. SHERIDAN, JR.,

Plaintiff,

v.

U.S. OFFICE OF PERSONNEL MANAGEMENT,

Defendant.

Case No. 16-cv-805 (KBJ)

MEMORANDUM OPINION

Pro se plaintiff Ronald L. Sheridan seeks access to the computer software that the Office of Personnel Management ("OPM") uses to administer background investigations to applicants for federal government jobs. (*See* Compl., ECF No. 1, ¶ 8.) Sheridan submitted a records request to OPM in April of 2015, asking for "[c]omputer files containing the source code" for the agency's Electronic Questionnaires for Investigations Processing ("e-QIP") system, as well as related "design and operations documentation for e-QIP." (*Id.* ¶ 9.) Sheridan filed the instant lawsuit after OPM failed to respond to his request; he invokes the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and asks this Court to declare OPM's withholding "unlawful" and to order OPM to produce the requested records "without further delay." (*Id.*, Prayer for Relief, ¶¶ C–D.)

Before this Court at present are the parties' cross-motions for summary judgment. (*See* Mem. in Supp. of Def.'s Mot. for Summ. J. ("Def.'s Mem."), ECF No. 8; Pl.'s Mem. in Opp'n to Def.'s Mot. for Summ. J. & in Supp. of Pl.'s Cross-Mot. for

Summ. J. ("Pl.'s Mem."), ECF No. 11.) In its motion, OPM argues that the e-QIP source code and related documentation are exempt from disclosure under the FOIA pursuant to Exemption 7(E), 5 U.S.C. § 552(b)(7)(E), because the e-QIP source code and related documentation were compiled for a "law enforcement purpose" (*see* Def.'s Mem. at 11–12), and producing those records could reasonably be expected to increase the risk that undeserving individuals might successfully navigate the background investigation process, and also the risk that the e-QIP system will be the target of cyber-intrusion (*see id.* at 12–13).[1] OPM further argues that because Exemption 7(E) applies to the requested records in their entirety, no reasonably segregable, non-exempt portions of those records can be produced to Sheridan (*see id.* at 15–16), and that even if some portions of the requested records are segregable, they would nevertheless be exempt from disclosure pursuant to FOIA Exemption 2, which encompasses "matters that are . . . related solely to the internal personnel rules and practices of an agency[,]" 5 U.S.C. § 552(b)(2). (*See* Def.'s Mem. at 13–15.) For his part, Sheridan maintains that neither Exemption 7(E) nor Exemption 2 applies (*see* Pl.'s Mem. at 10–15), and that even if they do, OPM has not adequately complied with the FOIA's segregability requirement (*see id.* at 15).

Although Sheridan's written and oral presentation in regard to this matter was exceptional for a non-lawyer advocate, for the reasons explained below, this Court agrees with OPM that the requested records are exempt from disclosure pursuant to Exemption 7(E), and that OPM has adequately complied with its obligation to identify

[1] Page-number citations to documents the parties have filed refer to the page numbers that the Court's electronic filing system automatically assigns.

and produce any reasonably segregable, non-exempt portions of the requested records. Accordingly, OPM's motion for summary judgment will be **GRANTED** and Sheridan's cross-motion for summary judgment will be **DENIED**. A separate Order consistent with this Memorandum Opinion will follow.

I. BACKGROUND[2]

"OPM functions as the human resources service provider for Federal agencies in the executive branch and, as part of that function, provides over 90% of the Government's background investigations, conducting over two million investigations a year." (Def.'s Statement of Material Facts Not in Genuine Dispute ("Def.'s SOMF"), ECF No. 8, ¶ 2; *see also* Decl. of Lawrence W. Anderson ("Anderson Decl."), ECF No. 8-2, ¶ 21.) OPM's authority to conduct background investigations derives from multiple statutes, *see, e.g.*, 5 U.S.C. § 1304(a); 22 U.S.C. § 272b, as well as from an Executive Order that requires background investigations in order to ensure that all federal government employees are "reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States[.]" Exec. Order No. 10,450, 3 C.F.R. 936 (1949–1953 Comp.). "The principal purpose of a background investigation is to ensure that a prospective employee has not broken the law or engaged in other conduct making her ineligible for the position." *Mittleman v. OPM*, 76 F.3d 1240, 1243 (D.C. Cir. 1996).

To conduct its work, OPM uses the e-QIP system, "which provides secure, web-based access for applicants to enter, update, and transmit" various background

[2] The facts that are recited in this Memorandum Opinion are not in dispute. (*See* Pl.'s Resp. to Def.'s Statement of Material Facts Not in Genuine Dispute, ECF No. 11, ¶¶ 1–5.)

investigation forms. (Def.'s SOMF ¶ 3; *see also* Anderson Decl. ¶ 14.) Individuals use these forms to provide information regarding matters such as foreign contacts and financial and criminal histories. (*See* Def.'s SOMF ¶ 4; Anderson Decl. ¶ 15.) Blank versions of background investigation forms are publicly available[3]; however, applicants can only complete and submit these forms through e-QIP at the invitation of a sponsoring agency. (*See* Def.'s SOMF ¶ 5; Anderson Decl. ¶ 15.) The e-QIP system "allow[s] individuals to complete the appropriate investigative form and transmit the data through the requesting Government agency to OPM's central computer system." (Anderson Decl. ¶ 16.) Thus, the system is also "designed to house the completed personnel security investigative forms." (Def.'s SOMF ¶ 5.)

On April 15, 2015, Sheridan submitted a FOIA request to OPM, requesting "[c]omputer files containing the source code to the Office of Personnel Management's 'Electronic Questionnaires for the Investigations Processing (e-QIP)' application and computer files or hardcopy records containing design and operations documents for e-QIP." (Def.'s SOMF ¶ 1.) After emailing twice for a status update to no avail (*see* Compl. ¶¶ 14–15; Exs. 3–4 to Anderson Decl.), Sheridan treated the agency's lack of responsiveness as a "constructive denial" and filed an administrative appeal on February 1, 2016. (Compl.¶ 23; *see also* Ex. 7 to Anderson Decl.) To date, OPM has not issued any formal response to Sheridan's appeal. (*See* Compl. ¶ 26; Def.'s Answer to Pl.'s Compl. ("Answer"), ECF No. 5, ¶ 26.) *See also* 5 U.S.C. § 552(a)(6)(C)(i) (providing for constructive exhaustion of administrative remedies).

[3] *See, e.g.*, *Standard Form 85P, Questionnaire for Public Trust Positions*, U.S. Office of Personnel Mgmt., https://www.opm.gov/forms/pdf_fill/SF85P.pdf (last visited Sept. 26, 2017).

On April 29, 2016, Sheridan filed the present lawsuit, alleging that OPM violated the FOIA by failing to respond to his document request and by failing to produce the requested documents. (*See* Compl. ¶¶ 27, 29.) Asserting claims under the FOIA, Sheridan seeks a declaration that OPM's failure to make a determination on whether or not to comply with his FOIA request within twenty working days, failure to respond to his administrative appeal within twenty working days, and failure to provide the requested records are unlawful. (*See id.*, Prayer for Relief, ¶¶ A–C.) Sheridan also asks the Court to order OPM to produce the requested records and award him litigation costs. (*See id.*, Prayer for Relief, ¶¶ D–E.)

The parties have filed cross-motions for summary judgment under Federal Rule of Civil Procedure 56 that are now ripe for this Court's review.[4] OPM's motion reports that the agency has searched for the records that Sheridan requested and has located several responsive items: specifically, the e-QIP source code (which is purportedly stored across 3,241 different electronic files), and also a 79-page design manual and a 109-page operations manual. (*See* Def.'s Mem. at 9; Anderson Decl. ¶¶ 18–19.)[5] However, OPM has declined to produce these records to Sheridan, and it argues that its withholding is justified because the records are exempt from the FOIA under Exemption 7(E), which protects from disclosure certain "'records or information compiled for law enforcement purposes'" if such disclosure might risk compromising an agency's law

[4] *See* Def.'s Mem.; Pl.'s Mem.; Combined Reply Mem. in Supp. of Def.'s Mot. for Summ. J. and in Opp'n to Pl.'s Cross-Mot. ("Def.'s Reply"), ECF No. 13; Pl.'s Reply in Supp. of Pl.'s Cross-Mot. for Summ. J. ("Pl.'s Reply"), ECF No. 15.

[5] Courts in this District have previously held that computer program files constitute "records" as that term is used in the FOIA, *see,e.g.*, *Cleary, Gottlieb, Steen & Hamilton v. Dep't of Health & Human Servs.*, 844 F. Supp. 770, 782 (D.D.C. 1993), and OPM does not argue to the contrary in this case (*see* Hrg. Tr. at 3–4).

enforcement function. (Def.'s Mem. at 12 (quoting 5 U.S.C. § 552(b)(7)(E)).) OPM argues that, because the agency uses e-QIP to process background-investigation information, the agency's disclosure of the system's source code, structure, and operation would render e-QIP vulnerable to hacking and phishing, and would also enable undeserving individuals to pass the background-check process successfully. (*See* Def.'s Mem at 11–13.) In making this argument, OPM further contends that "Exemption 7(E) applies to *all* of the requested information and that non-exempt material could not be segregated in a manner that would provide meaningful information." (*Id.* at 16 (emphasis added).) In the alternative, OPM argues that even assuming that some of the requested information "is not subject to Exemption 7(E), and that any such information could be segregated in a meaningful manner from the rest of the requested information, that same information [would be] subject to Exemption 2" (*id.*), which protects from disclosure matters that are "related solely to the internal personnel rules and practices of an agency[.]" 5 U.S.C. § 552(b)(2). In OPM's view, Exemption 2 encompasses any segregable information in the requested records, because the records relate to hiring practices and because there is no legitimate public interest in the e-QIP source code. (*See* Def.'s Mem. at 13–15.)

In his cross-motion, Sheridan responds to each of OPM's arguments in turn. With respect to Exemption 7(E), Sheridan argues that the requested records are not exempt because there "would be no harm in their disclosure[,]" in light of the fact that "[u]nderstanding the information collected by e-QIP does not provide an applicant with any more information about the investigation adjudication process than simply reading the paper forms" that are already publicly available. (Pl.'s Mem. at 12.) During the

Court's motion hearing, Sheridan added that even if certain portions of the e-QIP source code might reveal aspects of how background investigations are processed and adjudicated—one of OPM's stated concerns—it is likely that other, segregable portions of the code would not implicate that concern, because source code is often stored in separate "modules" that perform different functions, and OPM's representation that the e-QIP code is stored across "3,241 source code files" (*see* Anderson Decl. ¶ 18) suggests that that is the case here. (*See* Hrg. Tr. at 38–39.) Finally, with respect to Exemption 2, Sheridan argues that even assuming, *arguendo*, that OPM has correctly characterized e-QIP as pertaining to the "internal personnel rules and practices of an agency[,]" 5 U.S.C. § 552(b)(2), Exemption 2 does not cover the requested records because that exemption is inapplicable when there is a "'genuine and important public interest'" in the records (Pl.'s Mem. at 13 (quoting *Dep't of the Air Force v. Rose*, 425 U.S. 352 (1976))), and in this case, "there are significant benefits to both the public and the government when source code can be shared" because "source code can be re-used, re-purposed, and improved" (*id.* at 14).[6] The Court held a hearing on the parties' cross-motions on July 25, 2017. (*See* Min. Entry of July 25, 2017.)

II. LEGAL STANDARDS

A. Summary Judgment In The FOIA Context

FOIA cases typically are decided on motions for summary judgment. *See Liberman v. U.S. Dep't of Transp.*, 227 F. Supp. 3d 1, 8 (D.D.C. 2016). Summary judgment is warranted when "the movant shows that there is no genuine issue as to any

[6] Sheridan's cross-motion also argues that OPM did not conduct an adequate search in response to his FOIA request (*see* Pl.'s Mem. at 9–10), but he expressly abandoned this argument during the Court's motion hearing (*see* Hrg. Tr. at 48–49).

material fact and the movant is entitled to a judgment as a matter of law." Fed. R. Civ. P. 56(a). "In a FOIA case, summary judgment may be granted to the government if the agency proves that it has fully discharged its obligations under the FOIA, after the underlying facts and the inferences to be drawn from them are construed in the light most favorable to the FOIA requester." *Media Research Ctr. v. U.S. Dep't of Justice*, 818 F. Supp. 2d 131, 136–37 (D.D.C. 2011) (internal quotation marks and citation omitted).

B. Exemption 7(E)

The FOIA "mandates that an agency disclose records on request, unless they fall within one of nine exemptions." *Milner v. Dep't of Navy*, 562 U.S. 562, 565 (2011). "An agency that has withheld responsive documents pursuant to a FOIA exemption can carry its burden to prove the applicability of the claimed exemption by affidavit, and [courts] review the agency's justifications therein *de novo*." *Larson v. Dep't of State*, 565 F.3d 857, 862 (D.C. Cir. 2009). One of these exemptions—'Exemption 7'—permits an agency to withhold "records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information" would result in one of several enumerated harms. 5 U.S.C. § 552(b)(7). One of the listed harms—codified in subsection (E) of section 552(b)(7)—is implicated where the agency's production of law enforcement 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[.]" 5 U.S.C. § 552(b)(7)(E). Thus, the text of Exemption 7(E) appears to permit an agency to withhold records only if certain criteria are satisfied: (1) the records were "compiled for law enforcement purposes," (2) production of the records "would disclose" either "techniques and procedures for law enforcement investigations or prosecutions" or "guidelines for law enforcement investigations or prosecutions[,]" and (3) "such disclosure could reasonably be expected to risk circumvention of the law[.]" *Id.*; *see also Sack v. U.S. Dep't of Def.*, 823 F.3d 687, 693–94 (D.C. Cir. 2016).

The requirement that records have been "compiled for law enforcement purposes" can be satisfied "even when the materials have not been compiled in the course of a specific investigation." *Tax Analysts v. IRS*, 294 F.3d 71, 79 (D.C. Cir. 2002). "Law enforcement entails more than just investigating and prosecuting individuals *after* a violation of the law[,]" *Pub. Emps. For Envtl. Responsibility v. U.S. Section, Int'l Boundary and Water Comm'n*, 740 F.3d 195, 203 (D.C. Cir. 2014) (emphasis in original); it also includes "'proactive steps designed to prevent criminal activity and to maintain security.'" *Id.* (quoting *Milner*, 562 U.S. at 582 (Alito, J., concurring)). Moreover, "[t]he term 'law enforcement' in Exemption 7 refers to the act of enforcing the law, both civil and criminal." *Id.*

The requirement that records "would disclose techniques and procedures for law enforcement investigations or prosecutions," 5 U.S.C. § 552(b)(7)(E), is met, *inter alia*, where a record would disclose details about a law enforcement technique or procedure itself, *see Blackwell v. FBI*, 646 F.3d 37, 42 (D.C. Cir. 2011) (forensic examination of a computer); *Sack*, 823 F.3d at 694 (polygraphs), or would disclose information regarding "when . . . agencies are likely to employ" certain techniques or procedures, *Sack*, 823 F.3d at 694. And it is also satisfied if the record would disclose assessments about whether certain techniques or procedures "are effective." *Id.*

The final element of Exemption 7(E)—*i.e.*, the requirement that disclosure of a record "could reasonably be expected to risk circumvention of the law," 5 U.S.C. § 552(b)(7)(E)—"sets a relatively low bar for the agency to justify withholding[.]" *Blackwell*, 646 F.3d at 42. In fact, "the exemption looks not just for [actual] circumvention of the law, but for a risk of circumvention; not just for an actual or certain risk of circumvention, but for an expected risk; not just for an undeniably or universally expected risk, but for a reasonably expected risk; and not just for certitude of a reasonably expected risk, but for the chance of a reasonably expected risk." *Mayer Brown LLP v. IRS*, 562 F.3d 1190, 1193 (D.C. Cir. 2009). Consequently, "[r]ather than requiring a highly specific burden of showing how the law will be circumvented, exemption 7(E) only requires that the [agency] demonstrate[] logically how the release of [the requested] information might create a risk of circumvention of the law." *Id.* at 1194 (third and fourth alterations in original) (internal quotation marks and citation omitted).

C. Exemption 2

FOIA Exemption 2 protects "matters that are . . . related solely to the internal personnel rules and practices of an agency." 5 U.S.C. § 552(b)(2). "An agency's 'personnel rules and practices' are its rules and practices dealing with employee relations or human resources." *Milner*, 562 U.S. at 570. The "rules and practices" referenced in Exemption 2 "concern the conditions of employment in federal agencies—such matters as hiring and firing, work rules and discipline, compensation and benefits." *Id.* And to be covered by Exemption 2, these matters must be "internal," which means that "the agency must typically keep the records to itself for its own use."

Id. at 570 n.4. Finally, Exemption 2 only encompasses those matters that relate "solely" to an agency's internal rules and practices, 5 U.S.C. § 552(b)(2), which means that it does not exempt "matters [that are] subject to . . . a genuine and significant public interest[.]" *Dep't of the Air Force v. Rose*, 425 U.S. at 369; *see also Shapiro v. U.S. Dep't of Justice*, 153 F. Supp. 3d 253, 278 (D.D.C. 2016) (explaining that the "public interest" limitation from *Rose* survives the Supreme Court's more recent decision in *Milner*).

D. Segregability

The FOIA "requires that even if some materials from the requested record are exempt from disclosure, any 'reasonably segregable' information from those documents must be disclosed after redaction of the exempt information unless the exempt portions are 'inextricably intertwined with exempt portions.'" *Johnson v. Exec. Office of U.S. Attorneys*, 310 F.3d 771, 776 (D.C. Cir. 2002) (quoting 5 U.S.C. § 552(b)). "In order to demonstrate that all reasonably segregable material has been released, the agency must provide a detailed justification for its non-segregability." *Id.* (internal quotation marks and citation omitted). "However, the agency is not required to provide so much detail that the exempt material would be effectively disclosed." *Id.* "Agencies are entitled to a presumption that they complied with the obligation to disclose reasonably segregable material." *Sussman v. U.S. Marshals Serv.*, 494 F.3d 1106, 1117 (D.C. Cir. 2007).

III. ANALYSIS

OPM argues that it properly withheld the e-QIP computer source code and related design and operation documents under Exemption 7(E), and in the alternative, Exemption 2, and that there is no reasonably segregable, non-exempt information that is not inextricably intertwined with exempt information. As explained fully below, the Court agrees with OPM that Exemption 7(E) applies to the requested records in this case, and the Court also concludes that OPM has satisfied its burden of demonstrating that the requested records do not contain any reasonably segregable, non-exempt information.[7]

A. OPM Properly Withheld The Requested Records Under Exemption 7(E)

As explained above, Exemption 7(E) allows an agency to withhold "records or information compiled for law enforcement purposes, but only to the extent that production 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[.]" 5 U.S.C. § 552(b)(7)(E). The Court agrees with OPM that the e-QIP source code and related design and operation documents were created for law-enforcement purposes, and that releasing those documents could reasonably be expected to increase two risks, both of which relate to circumvention of the law: the risk that undeserving job applicants will evade the background-investigation process, and the risk of cyber-intrusion into OPM's electronic files.

1. The Requested Records Were "Compiled For Law Enforcement Purposes"

The core objectives of OPM's background-investigation function are to "ensure that a prospective employee has not broken the law or engaged in other conduct making

[7] Because the Court concludes that the requested records are exempt from disclosure in their entirety under Exemption 7(E), the Court does not evaluate whether Exemption 2 applies as well.

her ineligible for the position[,]" and to "determine whether there are any law enforcement or security issues in [her] past that could affect [her] ability . . . to carry out the position." *Mittleman*, 76 F.3d at 1243 (second, third, and fourth alterations in original) (internal quotation marks and citation omitted). The D.C. Circuit has long held that these are "law enforcement purposes" within the meaning of FOIA Exemption 7. *See Morley v. CIA*, 508 F.3d 1108, 1128 (D.C. Cir. 2007) ("Background investigations conducted to assess an applicant's qualification . . . inherently relate to law enforcement."). Indeed, in *Mittleman*, the Circuit specifically held that OPM properly withheld certain responsive documents that it compiled in the course of performing an individual job applicant's background investigation, *see* 76 F.3d at 1242, reasoning that, because OPM had compiled the requested records in service of the objective of conducting a background check, the records had been "compiled for law enforcement purposes" and thus were properly withheld under Exemption 7.[8]

Sheridan attempts to distinguish *Mittleman* on the grounds that that case "addressed background investigation information itself, not the tools or processes that support the background investigation process." (Pl.'s Mem. at 11.) Sheridan is correct that *Mittleman* addressed OPM's withholding of information from a particular individual's background-investigation file—and in fact, only certain information from that file (*i.e.*, the identities of two confidential sources that OPM consulted during the background investigation process, *see* 76 F.3d at 1242)—but this Court discerns no meaningful difference between records that are collected during a background

[8] Although *Mittleman* addressed the applicability of Exemption 7(D), not 7(E), both subsections of Exemption 7 require the agency to demonstrate that the requested records were "compiled for law enforcement purposes[.]" 5 U.S.C. § 552(b)(7)(D)–(E).

investigation and records that are related to the background-investigation system generally when it comes to the question of whether those records "were compiled for law enforcement purposes[.]" 5 U.S.C. § 552(b)(7). Indeed, the compilation requirement can be satisfied "even when the materials have not been compiled in the course of a specific investigation." *Tax Analysts*, 294 F.3d at 79. And in a case that concerned the disclosure of "[t]he CIA's security clearance techniques[,]" which "involve a general process applied to all background investigations of its officers[,]" the D.C. Circuit considered the statutory requirement to have been met, on the theory that "[b]ackground investigations conducted to assess an applicant's qualification . . . inherently relate to law enforcement." *Morley*, 508 F.3d at 1128–29; *see also, e.g.*, *Sack*, 823 F.3d at 694 (concluding that "reports about polygraph use were compiled for law enforcement purposes[,]" in part on the grounds that agencies use polygraphs during background investigations of job applicants).

Similarly, here, there is no dispute that the e-QIP source code and the related design and operations manuals exist to serve OPM's background-investigation function. Therefore, this Court has little trouble concluding that records concerning the e-QIP source code and related design and operation manuals were "compiled for law enforcement purposes" for the purpose of section 552(b)(7). (*See* Def.'s Mem. at 11–12.)

2. Producing The Requested Records "Would Disclose Techniques And Procedures For Law Enforcement Investigations Or Prosecutions"

The Court also agrees with OPM that the requested records "would disclose techniques and procedures for law enforcement investigations or prosecutions[.]" 5 U.S.C. § 552(b)(7)(E). (*See* Def.'s Mem. at 13.) The agency's affidavit explains that the e-QIP system "provides secure, web-based access for applicants to enter, update, and transmit electronic versions of" various background investigation forms. (Anderson Decl. ¶ 14.) The affidavit further explains that "[t]he source code and related operations and design manuals created for the system serve[] as an architectural diagram or roadmap of e-QIP." (*Id.* ¶ 29.) Furthermore and notably, the agency's affiant asserts that the source code reveals "*how* the data is analyzed [by OPM]," including "what types of information triggers further investigation, [and] which data fields are compared to search for inconsistencies[.]" (*Id.* ¶ 31 (emphasis added).) These assertions clearly support OPM's argument that the requested records would reveal law enforcement "techniques and procedures." *See Sack*, 823 F.3d at 694 (holding that reports about agency use of polygraph tests during background investigations would disclose law enforcement "techniques and procedures themselves, including when the agencies are likely to employ" polygraphs); *Blackwell v. FBI*, 646 F.3d 37, 42 (D.C. Cir. 2011) (holding that "details about procedures used during the forensic examination of a computer by an FBI forensic examiner . . . are undoubtedly 'techniques' or 'procedures' used for 'law enforcement investigations'" (internal quotation marks and citation omitted)).

3. Producing The Requested Records "Could Reasonably Be Expected To Risk Circumvention Of The Law"

Under the most natural reading of Exemption 7(E), this Court's analysis would end with its conclusions that the requested records were "compiled for law enforcement purposes" (*see supra* Part III.A.1), and that producing the records would disclose investigative "techniques and procedures" (*see supra* Part III.A.2), because, in this Court's view, the plain text of Exemption 7(E) establishes that if a record satisfies those two criteria, then the agency is entitled to withhold it without needing to further demonstrate that disclosure might risk circumvention of the law. *See* 5 U.S.C. § 552(b) ("This section does not apply to matters that are . . . (7) records or information compiled for law enforcement purposes, but only to the extent that production of such law enforcement records or information . . . (E) would disclose techniques or 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[.]"). The text separately references the disclosure of "techniques and procedures" on the one hand, and the disclosure of "guidelines" on the other, and mentions risk of "circumvention of the law" only with respect to the latter. *Cf. Lockhart v. United States*, 136 S. Ct. 958, 962–63 (2016) (discussing the "last antecedent" canon of interpretation).

Nevertheless, there appears to be "some disagreement" among courts about "whether the 'risk of circumvention' requirement applies to records containing 'techniques and procedures' or only to records containing 'guidelines.'" *Citizens for Responsibility & Ethics in Wash. v. Dep't of Justice*, 746 F.3d 1082, 1102 n.8 (D.C. Cir. 2014); *accord Pub. Emps.*, 740 F.3d at 204 n.4. Indeed, in at least two recent decisions reviewing agency withholdings under Exemption 7(E), the D.C. Circuit has proceeded to evaluate whether production of certain records could risk circumvention of the law, even after concluding that the records "were compiled for law enforcement purposes" and would disclose law enforcement "techniques and procedures." *See Sack*, 823 F.3d at 694–95; *Blackwell*, 646 F.3d at 42. Thus, out of an abundance of caution, this Court will now do the same.

As mentioned above, the burden of establishing that producing the requested records "could reasonably be expected to risk circumvention of the law," 5 U.S.C. § 552(b)(7)(E), is relatively easy to shoulder, because "[r]ather than requiring a highly specific burden of showing how the law will be circumvented, exemption 7(E) only requires that the [agency] demonstrate logically how the release of [the requested] information might create a risk of circumvention of the law." *Mayer Brown LLP*, 562 F.3d at 1194 (third alteration in original) (internal quotation marks and citation omitted). Here, OPM's affiant maintains that there is a risk that "[a]n individual seeking to circumvent the background investigation process could use the source code" to "leverage knowledge of the methods [by which] the data is analyzed to circumvent the law." (Anderson Decl. ¶ 31.) In this regard, the affidavit specifically asserts that such an individual could "find out how the data is analyzed, what types of information triggers further investigation, [and] which data fields are compared to search for inconsistencies" (*id.*), and that "[a]ccess to all o[r] part of the e-QIP source code and design documents would provide [such] an individual the roadmap to manipulate this intricate computer software when [the government is] conducting personnel investigations for new and current employees" (*id.* ¶ 33).

These are logical risks of exactly the sort that Exemption 7(E) empowers agencies to avoid. *See Morley*, 508 F.3d at 1129 ("It is self-evident that information revealing security clearance procedures could render those procedures vulnerable and weaken their effectiveness at uncovering background information on potential candidates."); *see also Mayer Brown LLP*, 562 F.3d at 1192 (stating that if a record contained "the words most likely to trigger increased surveillance during a wiretap," then "the applicability of [Exemption 7(E)] would be obvious"). In fact, in *Morley*, the D.C. Circuit concluded that an agency had demonstrated the requisite logical risk of circumvention of the law with an affidavit that stated merely "that release of th[e] information could 'provide insight' into the [agency's] security clearance procedure," 508 F.3d at 1129, and OPM has gone far beyond that in the instant case. Thus, OPM has carried its burden of demonstrating that producing the requested records could reasonably be expected to risk circumvention of the law based on the logical possibility that applicants for federal jobs might glean information about how background investigation forms are processed and use that information to pass their background checks undeservedly.

If that were not enough, OPM's affidavit also highlights risks related to cyber-intrusion that could materialize if the requested records are produced. First, the affidavit contends that producing the e-QIP source code and related manuals could increase the risk that a malicious actor might hack into the e-QIP system and access confidential data from completed background investigation forms. (*See* Anderson Decl. ¶¶ 28–29.) In particular, the affidavit notes that, "[a]lthough Plaintiff's request does not cover the individual records in the e-QIP system, because the system is both an interface for entering individuals' records and a data repository for the records, divulging the requested information renders the data housed in the system vulnerable as well." (*Id.* ¶ 28.) In its briefing, OPM points out that this risk "is more than hypothetical[,]" because "OPM has previously been the subject of cyber-intrusions that impacted background investigation records similar to the information contained in the e-QIP system." (Def.'s Mem. at 13.) In addition, and relatedly, OPM's affidavit contends that releasing the e-QIP source code and design and operations manuals could increase the risk of a phishing scam—a form of identity theft in which a malicious actor tricks an unwitting victim into divulging personal identifying information by mimicking a trusted entity. (*See* Anderson Decl. ¶ 30.) *See generally* Jennifer Lynch, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks,* 20 Berkeley Tech. L.J. 259 (2005). In this regard, OPM's affidavit specifically posits that

> if someone has the e-QIP source code and intend[s] to circumvent the law, that individual can determine what the system looks like to [a] customer organization. In this case the individual would have no need to breach e-QIP, [because] they could work to 'make themselves look like e-QIP' for the purposes of attacking a customer organization system.

(Anderson Decl. ¶ 30.) These additional cyber-intrusion risks further support the Court's conclusion that the agency has sufficiently demonstrated that producing the requested records "could reasonably be expected to risk circumvention of the law[.]" 5 U.S.C. § 552(b)(7)(E); *see Long v. Immigration & Customs Enf.*, 149 F. Supp. 3d 39, 51 (D.D.C. 2015) (noting that "courts in this District have recognized the risk of a cyber-attack or a breach of a law enforcement database as valid grounds for withholding under Exemption 7(E)").

Sheridan offers two vigorous rebuttals to OPM's arguments regarding a risk of circumvention of the law under the stated circumstances, but ultimately neither is persuasive. First, Sheridan contends that OPM's own description of the functionality of the e-QIP system does not substantiate the risks that OPM highlights. (*See* Pl.'s Mem. at 11–12.) For example, Sheridan says that because "[t]he description of e-QIP provided by the Defendant makes no mention of the implementation of any investigatory process, or for that matter any function of e-QIP beyond simple collection and transmission of information that was formerly collected on publicly available paper forms[,]" e-QIP likely functions as a mere repository such that producing the requested records could not possibly create a risk of job applicants cheating the background check process. (*Id.* at 11 (citing Anderson Decl. ¶¶ 14–16).) Sheridan adds that "no e-QIP functionality is described that would be used to *evaluate* the applicant's submitted information or execute any process designed to actually *adjudicate* the clearance request." (*Id.* (emphasis added).) But this account undervalues the specific statement of OPM's affiant that the requested records could reveal "how the data is analyzed, what types of information triggers further investigation, [and] which data fields are compared to search for inconsistencies" (Anderson Decl. ¶ 31), each of which implicates aspects of the agency's evaluation process in a manner that transcends a mere storage function. And in the absence of any contrary evidence in the record or blatant inconsistencies in OPM's affidavit, this Court must credit OPM's assessment of what processes the requested records would reveal. *See Mayer Brown LLP*, 562 F.3d at 1193 (describing the low burden that an agency must meet to demonstrate a risk of circumvention of the law); *see also Clemente v. FBI*, 867 F.3d 111, 117 (D.C. Cir. 2017) (noting courts' "presumption that agency affidavits are made in good faith").

Second, Sheridan takes issue with the cyber-intrusion-related risks that OPM posits, on the grounds that those risks are present anyway and would not be meaningfully increased if the e-QIP source code and related documents became public. (*See* Pl.'s Mem. at 13.) In support of this theory, Sheridan submits the affidavit of Karim Said, "an information security professional currently employed by NASA[,]" who has performed a security risk assessment of the e-QIP system based on publicly available information, and has concluded that "there is no significant difference in risk to the e-QIP information system posed by releasing the source code to e-QIP" because there are tools already available that malicious actors can use to compromise computer software in many circumstances. (Decl. of Karim A. Said, Ex. to Pl.'s Mem., ECF No. 11, ¶¶ 1, 23). To underscore this point, Sheridan emphasizes that the *previous* hack that OPM admittedly experienced (*see* Def.'s Mem. at 13 (referencing prior hack as evidence that the cyber-intrusion risk is real)) "was performed, notably, without access to the source code to the system." (Pl.'s Mem. at 13.) Thus, says Sheridan, OPM already has inadequate cyber defenses, so protecting the requested source code from disclosure in order to guard against cyber-intrusion is like "insisting that we lock the front door even though the back door is wide open[.]" (Hrg. Tr. at 68.)

These arguments appeal to basic common sense and are entirely rational. But the law requires more: courts must account for the language and purposes of a statute as precedents have interpreted it, and it is by now well established that an agency that invokes Exemption 7(E) need not show that an identified risk will actually increase substantially, or that the risks it relies upon will necessarily come to fruition; rather, "exemption 7(E) only requires that the [agency] demonstrate *logically* how the release of [the requested] information *might* create a risk of circumvention of the law." *Mayer Brown LLP*, 562 F.3d at 1194 (emphasis added) (second alteration in original) (internal quotation marks and citation omitted).

This Court is satisfied that OPM has done so here. The agency contends unequivocally that "releasing [the] source code [even] for systems that leverage the most up-to-date security sensitive features increases the risk of malicious activities for those systems[,]" and that "releasing the source code for older software is far worse." (Anderson Decl. ¶ 30.) It also maintains that, "at the very least[,]" a release of the e-QIP source code would "identify the 'locked doors' that have been designed into the software (telling a malicious actor where and how to attempt to breach a system)." (*Id.*) In this Court's view, the fact that a malicious actor does not need the help and could easily endeavor to find the key on his own (which is Sheridan's main point) does not rebut OPM's assertion that this disclosure would make the system easier to breach. Moreover, and in any event, the agency's assessment of cyber-intrusion risks reflects its access to more information than is available to either Sheridan or this Court, and is entitled to some deference. *See Long*, 149 F. Supp. 3d at 53 ("Judges are not cyber specialists, and it would be the height of judicial irresponsibility for a court to blithely disregard . . . a claimed risk" of "a cyber-attack on, or security breach of, an agency data system containing sensitive law enforcement and personal information."); *see also Levinthal v. FEC*, 219 F. Supp. 3d 1, 7 (D.D.C. 2016) (crediting FEC's contention that "information contained in the [requested records] could be used to gain unlawful access to the Commission's technology systems, obtain and manipulate sensitive and confidential data about candidates, officeholders, party committees, and others who interact with the Commission, or obtain and manipulate data stored within the Commission's systems regarding [Commission] enforcement matters" (second alteration in original)).

Therefore, upon consideration of all the arguments and evidence, this Court concludes that OPM has adequately demonstrated that the requested release carries potential risks of circumvention of the law.

B. OPM Has Made A Sufficient Showing That There Are No Reasonably Segregable, Non-Exempt Portions Of The Requested Records

Finally, this Court also agrees with OPM's contention that the FOIA entitles it to withhold the requested records in their entirety because there are no "reasonably segregable" portions of the e-QIP source code and related manuals. 5 U.S.C. § 552(b). OPM's affidavit asserts that "[p]roviding *any* of the information requested would allow an individual to have a blueprint of the" e-QIP system, and that "[a]ccess to all *or part* of the e-QIP source code and design documents would provide an individual the roadmap to manipulate this intricate computer software when conducting personnel investigations for new and current employees." (Anderson Decl. ¶ 33 (emphasis added).) *See also Levinthal*, 219 F. Supp. 3d at 7 (crediting assertion in agency affidavit that one of the requested records "'provides a blueprint to the Commission's networks' and that its public disclosure 'could thus enable hackers to bypass the Commission's current protection mechanisms'" (citation omitted)). "With respect to the source code" in particular, OPM's affidavit specifically asserts that "every portion of potentially nonexempt information is inextricably intertwined with exempt information, rendering review and release of only nonexempt portions very difficult, if not impossible to accomplish." (Anderson Decl. ¶ 34.) Furthermore, "[w]ith respect to the design and operations manuals Plaintiff has requested," the affidavit adds that "any portion of the detailed information contained in [those documents] could potentially and foreseeably be used to discover, map and target vulnerabilities in the system based on

. . . detailed knowledge of applications, servers, architecture, and controls." (*Id.* ¶ 35.) These are sufficiently "detailed justification[s]" for OPM's determinations regarding segregability to warrant deferring to OPM's decision to withhold the requested records in full. *Mead Data Cent. v. Dep't of the Air Force*, 566 F.2d 242, 261 (D.C. Cir. 1977).

Sheridan dismisses OPM's support for its segregability determination as "[m]ere conclusory statements[,]" and argues that OPM needed to say more in order to demonstrate that there are truly no reasonably segregable, non-exempt portions of the requested records. (Pl.'s Mot. at 15.) Specifically, Sheridan notes that "computer source code is generally organized in 'functions,' 'procedures,' or 'methods,' each of which generally perform a single specific task[,]" and he contends that "[s]uch structure lends itself to segregability" because, even if some portions of the source code might reveal investigative techniques, there will inevitably be at least some portions that do not. (Pl.'s Reply at 15.) During the motion hearing, Sheridan pointed to the fact that the e-QIP source code is stored across many different files as evidence that it exhibits exactly the sort of segregable structure that he describes. (*See* Hrg. Tr. at 38–39; *see also* Anderson Decl. ¶ 18 ("There are about 3,241 source code files that make up the system[.]").) But counsel for OPM persuasively responded that the risks of cyber-intrusion that it has identified—and in particular the risk of phishing—apply uniformly throughout the source code and related manuals, including to portions that would not otherwise be exempt because they do not themselves reveal investigative techniques. (*See* Hrg. Tr. at 59 ("[T]he more of those seemingly innocuous screens that [malicious actors] can replicate because they have the source code, the better and better that phishing exercise [and the] more effective it will be."); *see also* Anderson Decl. ¶¶ 34–35.)

All in all, the Court concludes that OPM has offered a sufficient and plausible explanation for its segregability decision, and Sheridan has not done enough to rebut the "presumption" that OPM "complied with the obligation to disclose reasonably segregable material." *Sussman*, 494 F.3d at 1117.

IV. CONCLUSION

Sheridan has requested the source code and related design and operations manuals for the e-QIP system, which OPM indisputably uses to facilitate the background investigations that it conducts for a huge swath of prospective federal government employees. According to OPM, producing these records could enable malicious actors to cheat the background investigation process or to engage in various forms of cyber-intrusion, and ultimately, this Court finds that argument persuasive. Specifically, this Court concludes that the requested records satisfy all of the requirements for withholding under Exemption 7(E), because the e-QIP source code and manuals were "compiled for law enforcement purposes," producing them "would disclose techniques and procedures for law enforcement investigations or prosecutions," and "such disclosure could reasonably be expected to risk circumvention of the law[.]" 5 U.S.C. § 552(b)(7)(E). The Court further concludes that OPM has satisfied its burden of establishing that these records can be withheld in full, because no "reasonably segregable" non-exempt information can be disclosed. *Id.* § 552(b).

Accordingly, as set forth in the accompanying Order, OPM's motion for summary judgment will be **GRANTED** and Sheridan's cross-motion for summary judgment will be **DENIED**.

Date: September 29, 2017

Ketanji Brown Jackson
KETANJI BROWN JACKSON
United States District Judge