

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

<p>Dave Levinthal, et al.,</p> <p style="padding-left: 40px;">Plaintiffs,</p> <p style="padding-left: 80px;">v.</p> <p>Federal Election Commission,</p> <p style="padding-left: 40px;">Defendant.</p>	<p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p>	<p>Civil No. 15-cv-01624 (APM)</p>
--	--	---

MEMORANDUM OPINION

I. INTRODUCTION

Plaintiffs Dave Levinthal and the Center for Public Integrity bring this suit under the Freedom of Information Act (“FOIA”). On July 6, 2015, Plaintiffs submitted a FOIA request to Defendant Federal Election Commission seeking: (1) a copy of a study that assesses vulnerabilities in the Commission’s information technology (“IT”) systems and makes recommendations to address those vulnerabilities; and (2) any emails and documents related to the study. Defendant produced non-exempt materials related to the study, but withheld the study itself. Plaintiffs brought this suit claiming that Defendant violated FOIA by failing to produce the study.

Upon consideration of the parties’ submissions and the record evidence, the court grants Defendant’s Motion for Summary Judgment and denies Plaintiffs’ Cross-Motion for Summary Judgment.

II. BACKGROUND

As required by Local Civil Rule 7(h)(1), Defendant Federal Election Commission (“Commission” or “Defendant”) submitted a detailed statement of undisputed material facts. *See* Def.’s Mot. for Summ. J., ECF No. 13 [hereinafter Def.’s Mot.], Def.’s Stmt. of Material Facts, ECF No. 13-1 [hereinafter Def.’s Stmt.]. Plaintiffs, for their part, responded with a bare-boned counter-statement that did not dispute Defendant’s factual assertions. Pls.’ Cross-Mot. for Summ. J., ECF No. 14 [hereinafter Pls.’ Mot.], Pls.’ Stmt. of Material Facts, ECF No. 14-1 [hereinafter Pls.’ Stmt.].¹ Accordingly, the court treats Defendant’s proffered facts, recited below, as conceded by Plaintiffs. *See SEC v. Banner Fund Int’l*, 211 F.3d 602, 616 (D.C. Cir. 2000) (“If the party opposing the motion fails to comply with [the] local rule, then ‘the district court is under no obligation to sift through the record’ and should ‘[i]nstead . . . deem as admitted the moving party’s facts that are uncontroverted by the nonmoving party’s Rule [LCvR 7.1(h)] statement.’” (alterations in original) (quoting *Jackson v. Finnegan, Henderson, Farabow, Garrett & Dunner*, 101 F.3d 145, 154 (D.D.C. 1996))).

A. Factual Background

In Fiscal Year 2014, the Commission hired an outside contractor, SD Solutions, LLC, to determine whether there were vulnerabilities in the Commission’s IT systems and, if there were, to provide remedial recommendations. Def.’s Stmt. ¶ 5; Def.’s Mot., Decl. of Alec Palmer, ECF No. 13-2 [hereinafter Palmer Decl.], ¶ 7. The Commission ordered the study to assist it in deciding whether to implement newly developed information security guidelines published by the U.S. Department of Commerce’s National Institute of Standards and Technology (“NIST”). Def.’s

¹ Plaintiffs later submitted a more fulsome statement of facts with their Reply Brief, *see* Pls.’ Reply, ECF No. 18, Pls.’ Stmt. of Genuine Issues of Fact, ECF No. 18-1, but that statement came too late, *see* LCvR 7(h)(1) (“[T]he Court may assume that facts identified by the moving party in its statement of material facts are admitted, unless such a fact is controverted in the statement of genuine issues filed *in opposition to the motion*.” (emphasis added)).

Stmt. ¶ 6; Palmer Decl. ¶ 7. In preparing its report, SD Solutions examined the Commission’s “physical and virtual information technology assets” and recommended measures for the Commission to protect its infrastructure from “wrongful interference, circumvention, or unlawful action by unauthorized persons.” Palmer Decl. ¶ 8. Furthermore, it assessed the “vulnerabilities to unlawful breach present in the Commission’s technological infrastructure, describing sensitive Commission systems and recommending specific security measures to address the vulnerabilities.” *Id.* The Commission refers to SD Solutions’ final report and its related documents, collectively, as the “NIST Study.” Def.’s Stmt. ¶ 8; Palmer Decl. ¶ 18.

The NIST Study consists of two parts. The first part is an overview memorandum prepared by the Commission’s Office of the Chief Information Officer. The overview memorandum lists measures the Office has used in the past to address IT vulnerabilities, summarizes SD Solutions’ final report, and discusses “the practicalities of implementing the [NIST] guidelines should the Commission adopt the recommendations in the Final Report.” Def.’s Stmt. ¶ 10; Palmer Decl. ¶¶ 2, 9, 10. The overview memorandum includes two appendices: (1) an abridged version of the full final report, and (2) a summary of both the recommendations in the report and the personnel and financial resources that would be required to satisfy each recommendation. *Id.* ¶¶ 10, 11.

The second part of the NIST Study is the final report itself. As discussed, the report describes the Commission’s IT network, assesses the security of each system and identifies the vulnerabilities therein, and contains recommendations for security measures to address the identified vulnerabilities. *Id.* ¶¶ 12, 14.

B. Procedural Background

Plaintiff Dave Levinthal is an investigative journalist employed by Plaintiff the Center for Public Integrity. *See* Pls.’ Mot. at 1; Def.’s Mot. at 3; Def.’s Stmt. ¶ 4. On July 6, 2015, Plaintiffs

submitted a FOIA request to the Commission, seeking: (1) “a copy of the 2015 National Institute of Standards and Technology Report—also known as the NIST study—pertaining to the Federal Election Commission’s operations,” and (2) “any FEC emails, memoranda, correspondence or other documents that, in any form or fashion, mention or refer to this National Institute of Standards and Technology report, by name or otherwise.” Def.’s Stmt. ¶ 38; Def.’s Mot., Decl. of Robert M. Kahn, ECF No. 13-3 [hereinafter Kahn Decl.], ¶ 6 & Ex. A [hereinafter FOIA Request].

On August 18, 2015, the Commission denied Plaintiffs’ request for a copy of the NIST Study, but granted their request for documents that mention or refer to the study, subject to applicable FOIA exemptions. Kahn Decl. ¶ 7 & Ex. C (Email from Robert M. Kahn to Dave Levinthal (Aug. 18, 2015)). The Commission eventually produced more than 1,450 pages of non-exempt records, and non-exempt portions of records, that mentioned or referred to the NIST Study. Jt. Status Rep., ECF No. 11.

Plaintiffs filed an administrative appeal challenging the decision to withhold the NIST Study, asserting that it “is likely to contain information that directly benefits the public’s understanding of Federal Election Commission capabilities and operations during a high-profile election season.” Kahn Decl. ¶ 8 & Ex. C. In September 2015, the Commission denied Plaintiffs’ appeal. *Id.* ¶ 10 & Ex. F (Email from Robert M. Kahn to Dave Levinthal (Sept. 30, 2015)).

Plaintiffs filed their Complaint in this court on October 5, 2015, challenging only Defendant’s non-disclosure of the NIST Study. *See* Compl., ECF No. 1. On March 17, 2016, Defendant filed a Motion for Summary Judgment, claiming that the NIST Study is exempt from disclosure both as a law enforcement record under FOIA Exemption 7(E) and as deliberative material under FOIA Exemption 5. Def.’s Mot. at 10–21. On April 8, 2016, Plaintiffs filed a Cross-Motion for Summary Judgment, which contests categorizing the NIST Study as a law

enforcement record under Exemption 7(E). *See* Pls.’ Mot at 4. Additionally, although Plaintiffs concede the applicability of Exemption 5, they argue that the Commission has failed to meet its obligation under FOIA to release any “reasonably segregable non-exempt information.” *Id.* at 5.

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). To make this determination, the court must “view the facts and draw reasonable inferences in the light most favorable to the [non-moving] party.” *Scott v. Harris*, 550 U.S. 372, 378 (2007) (internal quotation mark omitted). A dispute is “genuine” only if a reasonable factfinder could find for the nonmoving party, and a fact is “material” only if it is capable of affecting the outcome of litigation. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248–49 (1986). A non-material factual dispute cannot prevent the court from granting summary judgment. *Id.* at 249.

Most FOIA cases are appropriately decided on motions for summary judgment. *See Defenders of Wildlife v. U.S. Border Patrol*, 623 F. Supp. 2d 83, 87 (D.D.C. 2009). A court may award summary judgment in a FOIA case by relying on the information included in the agency’s affidavits or declarations if they are “relatively detailed and non-conclusory,” *SafeCard Servs., Inc. v. SEC*, 926 F.2d 1197, 1200 (D.C. Cir. 1991) (internal quotation marks omitted), and if they describe “the documents and the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemption, and are not controverted by either contrary evidence in the record nor by evidence of agency bad faith,” *Military Audit Project v. Casey*, 656 F.2d 724, 738 (D.C. Cir. 1981).

The agency bears the burden of demonstrating that each FOIA exemption applies, and its determinations are subject to de novo review in district court. *U.S. Dep’t of Justice v. Reporters*

Comm. for Freedom of the Press, 489 U.S. 749, 755 (1989) (citing 5 U.S.C. § 552(a)(4)(B)). To prevail on a motion for summary judgment, the agency must demonstrate that “each document that falls within the class requested either has been produced, is unidentifiable, or is wholly exempt from the Act’s inspection requirements.” *Goland v. Cent. Intelligence Agency*, 607 F.2d 339, 352 (D.C. Cir. 1978); *see also Students Against Genocide v. Dep’t of State*, 257 F.3d 828, 833 (D.C. Cir. 2001).

IV. DISCUSSION

A. FOIA Exemption 7(E)

The court first considers whether the NIST Study is exempt from disclosure under FOIA Exemption 7(E). Def.’s Mot at 10–17; Pls.’ Mot. at 3–4.

Under Exemption 7(E), an agency may withhold information (1) “compiled for law enforcement purposes” if (2) its release “would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions,” and (3) such “disclosure could reasonably be expected to risk circumvention of the law.” 5 U.S.C. § 552(b)(7)(E). Exemption 7(E) “sets a relatively low bar for the agency to justify withholding,” *Blackwell v. FBI*, 646 F.3d 37, 42 (D.C. Cir. 2011), and “where an agency ‘specializes in law enforcement, its decision to invoke [E]xemption 7 is entitled to deference,’” *Lardner v. Dep’t of Justice*, 638 F. Supp. 2d 14, 31 (D.D.C. 2009) (quoting *Campbell v. Dep’t of Justice*, 164 F.3d 20, 32 (D.C. Cir. 1998)). This does not excuse an agency, however, from the requirement of describing its “justifications for withholding the information n with specific detail.” *Am. Civil Liberties Union v. Dep’t of Def.*, 628 F.3d 612, 619 (D.C. Cir. 2011).

In this case, Plaintiffs offer a single argument challenging Defendant’s invocation of Exemption 7(E): the NIST Study was not “compiled for law enforcement purposes.” Pls.’ Mot. at 4.² The court has little trouble rejecting that contention.

A record is “compiled for law enforcement purposes” so long as there is (1) a rational “nexus” between the record and the agency’s law enforcement duties, and (2) a connection between the subject of the record and a possible security risk or violation of federal law. *See Campbell*, 164 F.3d at 32; *see also Pratt v. Webster*, 673 F.2d 408, 420 (D.C. Cir. 1982). The latter requirement must be satisfied “to establish that the agency acted within its principal function of law enforcement, rather than merely engaging in a general monitoring of individuals’ activities.” *Pratt*, 673 F.3d at 420. The NIST Study satisfies both requirements.

First, the NIST Study meets the rational “nexus” requirement because a federal agency, like the Commission, cannot effectively carry out its law enforcement function unless it has a secure and reliable IT system. The Commission is responsible for investigating violations of the Federal Election Campaign Act. *See* Def.’s Mot. at 5–6; Def.’s Stmt. ¶¶ 1–3; 52 U.S.C. § 30109(a)(1)–(2). Its IT system contains sensitive information related to investigations, including “subpoenas, requests for information and documents, reports of investigation, and responses to Commission-issued subpoenas and requests.” Palmer Decl. ¶ 17. The system also contains a “confidential scoring system, the Enforcement Priority System, which identifies significant cases for enforcement[.]” *Id.* ¶ 16. In short, the Commission’s IT system is central to its law

² The court, therefore, treats as conceded the remaining elements of Exemption 7(E)—namely, that the exempted record (1) “would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions” and (2), if disclosed, “could reasonably be expected to risk circumvention of the law.” 5 U.S.C. § 552(b)(7)(E). *See Wilkins v. Jackson*, 750 F. Supp. 2d 160, 162 (D.D.C. 2010) (“It is well established that if a plaintiff fails to respond to an argument raised in a motion for summary judgment, it is proper to treat that argument as conceded.”); *Sykes v. Dudas*, 573 F. Supp. 2d 191, 202 (D.D.C. 2008) (“[W]hen a party responds to some but not all arguments raised on a Motion for Summary Judgment, a court may fairly view the unacknowledged arguments as conceded.”).

enforcement function. *See id.* (“The Commission’s information systems network allows it to fulfill its statutory obligation to administer and enforce campaign finance laws.”).

The NIST Study in turn was designed to promote the integrity of that system and thus itself serves a law enforcement function. The study’s purpose was to “assess the vulnerabilities of the Commission’s information technology systems” and to make “recommendations about how the Commission could protect its systems from wrongful interference, circumvention, or unlawful action by authorized persons.” Palmer Decl. ¶¶ 7, 8. A study designed to evaluate and improve a critical law enforcement tool, such as an IT system, easily meets the rational nexus requirement.

Second, there is a connection between the NIST Study and a possible security risk or violation of federal law. According to the Commission’s Chief Information Officer, Alec Palmer, the NIST Study is the type of assessment “that, if publicly disclosed, could be used by persons with malicious objectives to do great harm.” *Id.* ¶ 19. Palmer asserts that “information contained in the NIST Study 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.” *Id.* Further, Palmer explains that a person with access to the NIST Study “could use the information contained [therein] to seriously threaten the Commission’s ability to fulfill its civil enforcement and other statutory duties.” *Id.* Finally, Palmer attests that the NIST Study “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.” *Id.* ¶ 21. This court observed in *Long v. Immigration and Customs Enforcement*, 149 F. Supp. 3d 39, 53 (D.D.C. 2015), that “[j]udges 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 or a security breach. The court will not disregard such risk in this case. Accordingly, the court finds that the NIST Study satisfies the second prong of the “compiled for law enforcement purposes” inquiry.

Plaintiffs offer two rejoinders. First, they contend that the NIST Study is not “compiled for a law enforcement purpose” because “[i]t is not connected to an investigation.” Pls.’ Mot. at 4. That argument misconstrues the law. The Court of Appeals consistently has held that records do not have to be linked to a specific investigation to be properly withheld under Exemption 7(E). For instance, in *Tax Analysts v. Internal Revenue Service (IRS)*, the court held that IRS materials related to law enforcement activities “outside of the context of a specific investigation” met the threshold for materials “compiled for law enforcement purposes” under Exemption 7(E). *See* 294 F.3d 71, 73, 78–79 (D.C. Cir. 2002). In so holding, it observed that Congress amended Exemption 7 in 1986 to make clear that 7(E) “was not limited to records or information addressing only individual violations of the law.” *Id.* at 79. More recently, in *Blackwell v. Federal Bureau of Investigation*, the Court of Appeals held that the FBI had properly withheld methods of data collection, organization, and presentation contained in certain reports under Exemption 7(E). 646 F.3d at 42. The methods were developed for the FBI to meet the agency’s “investigative needs,” rather than linked to a specific investigation. *Id.*

Moreover, as Defendant correctly points out, Def.’s Mot. at 11, 13–14, courts in this District repeatedly have held that information connected to law enforcement databases qualifies for exemption under 7(E). *See, e.g., Long*, 149 F. Supp. 3d at 44 (holding that requests for metadata and database schema of law enforcement information databases qualify for exemption under 7(E)); *Strunk v. U.S. Dep’t of State*, 905 F. Supp. 2d 142, 146–48 (D.D.C. 2012) (holding that computer transaction and function codes that reveal how to navigate and retrieve information from a law

enforcement database were properly withheld under Exemption 7(E)); *Miller v. U.S. Dep't of Justice*, 872 F. Supp. 2d 12, 29 (D.D.C. 2012) (holding that numerical codes used to identify information and individuals, as well as codes “relate[d] to procedures concerning the use of law enforcement resources and databases . . . [and] case program and access codes[,]” were properly withheld under Exemption 7(E)); *Skinner v. U.S. Dep't of Justice*, 893 F. Supp. 2d 109, 113–14 (D.D.C. 2012) (holding that user access codes that facilitated access to a law enforcement database were properly redacted under Exemption 7(E)), *aff'd sub nom. Skinner v. Bureau of Alcohol, Tobacco, Firearms & Explosives*, No. 12-5319, 2013 WL 3367431 (D.C. Cir. May 31, 2013)). Thus, the fact that the NIST Study does not pertain to a particular investigation does not place it outside Exemption 7(E).

Second, Plaintiffs argue that Exemption 7(E) is inapplicable because Defendant “has not established that the vulnerabilities described in the NIST Study still exist.” Pls.’ Mot. at 4. More specifically, Plaintiffs argue that, even if Exemption 7(E) applies “to portions of the NIST Study, to the extent that facts on the ground have changed since the preparation of the report, disclosure of previous vulnerabilities would not fall under Exemption 7(E).” *Id.* at 5. That argument is a nonstarter. Again, the Palmer Declaration, which the court described above, amply supports Defendant’s contention that the public release of the NIST Study—or any portion of it—would run the risk of compromising the Commission’s law enforcement function. According to Palmer, if released, unauthorized readers of the NIST Study could “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.” *Id.* ¶ 19. Additionally, Palmer states that an unauthorized individual or

government armed with the NIST Study could “seriously threaten the Commission’s ability to fulfill its civil enforcement and other statutory duties” and “alter the disclosure data that the Commission makes available on its public website, thereby providing false disclosure information that could adversely influence the outcome of an election.” *Id.* ¶¶ 19–20. Further, disclosing the NIST Study could allow hackers to gain access to the Commission’s networks, enabling them to “distort or prevent access to campaign finance reports,” or “expose sensitive information about parties regulated by the Commission.” *Id.* ¶¶ 21, 24. Palmer’s Declaration credibly demonstrates that disclosure of any portion of the NIST Study would pose a present and genuine security threat to the Commission’s law enforcement function. Accordingly, the court rejects Plaintiffs’ argument that the NIST Study is not exempt under 7(E).

B. FOIA Exemption 5 and Segregability

Defendant also invokes FOIA Exemption 5 to withhold the NIST Study. Def.’s Mot. at 17. Exemption 5 shields disclosure of “inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency.” 5 U.S.C. § 552(b)(5). Exemption 5 has been interpreted to incorporate the three traditional civil discovery privileges—the attorney work product privilege, the deliberative process privilege, and the attorney-client privilege. *Burka v. U.S. Dep’t of Health & Human Servs.*, 87 F.3d 508, 518 (D.C. Cir. 1996). Here, Defendant asserts the deliberate process privilege as the basis for invoking Exemption 5. Def.’s Mot. at 17–21; *see Tax Analysts v. IRS*, 117 F.3d 607, 616 (D.C. Cir. 1997) (describing the deliberative process privilege as covering records that are both “predecisional” and “deliberative”).

Plaintiffs do not contest the applicability of the deliberative process privilege to the NIST Study. *See* Pls.’ Mot. at 5 (“Plaintiffs do not doubt that the NIST Study contains predecisional

recommendations.”). Instead, they challenge whether Defendant has satisfied its duty to segregate and produce non-exempt factual material contained within the NIST Study. *Id.* Specifically, Plaintiffs argue that Defendant “has not established that [the factual material is] actually ‘inextricably entwined’ with deliberations.” *Id.*; see *Mead Data Cent., Inc. v. U.S. Dep’t of the Air Force*, 566 F.2d 242, 260 (D.C. Cir. 1977) (collecting cases and explaining that “[i]t has long been a rule in this Circuit that non-exempt portions of a document must be disclosed unless they are inextricably intertwined with exempt portions”). The court disagrees.

Because “the focus of FOIA is information, not documents . . . an agency cannot justify withholding an entire document simply by showing that it contains some exempt material.” *Mead Data Cent.*, 566 F.2d at 260. FOIA therefore requires that “[a]ny reasonably segregable portion of [the] record shall be provided to any person requesting such record after deletion of the portions which are exempt.” 5 U.S.C. § 552(b). An agency must provide a “detailed justification” and not just make “conclusory statements” to support its segregability determination. *Mead Data Cent.*, 566 F.2d at 261. Agencies, however, “are entitled to a presumption that they complied with the obligation to disclose reasonably segregable material,” which can be overcome by contrary evidence produced by the requester. *Sussman v. U.S. Marshals Serv.*, 494 F.3d 1106, 1117 (D.C. Cir. 2007).

The Palmer Declaration provides a “detailed justification” for the Commission’s decision that no part of the NIST Report is segregable, and Plaintiffs have not offered any evidence to the contrary. According to Palmer, the Commission’s Office of the Chief Information Officer conducted a line-by-line analysis of the NIST Study to determine if any portion could be segregated and released without jeopardizing the security of its networks. Palmer Decl. ¶¶ 25–27. Palmer observes that the “factual descriptions of the Commission’s information technology


systems and their vulnerabilities in the Final Report form the basis of the Report’s analysis[] . . . and they reflect the need for the recommended protocols that constitute the core of the NIST Study.” *Id.* ¶ 26. If the factual content of the NIST Study were publicly disclosed, Palmer explains, it “would effectively release many of the NIST Study’s recommendations, as well as the substance of the vulnerability analysis that [the Office of the Chief Information Officer] submitted to the Commission for its determination on whether to accept those recommendations.” *Id.* ¶ 27. “The factual descriptions expose the Commission to risk of a security breach of its network and information technology systems.” *Id.*

Palmer’s Declaration clearly establishes that the factual portions of the NIST Study are “inextricably intertwined” with its deliberative elements. *Mead Data Cent.*, 566 F.2d at 260. It also sets forth with “reasonable specificity” why those factual portions cannot be segregated. *Armstrong v. Exec. Office of the President*, 97 F.3d 575, 578–79 (D.C. Cir. 1996). Accordingly, the court rejects Plaintiffs’ argument that Defendant has not met its duty of segregability.

V. CONCLUSION

For the foregoing reasons, the court grants Defendant’s Motion for Summary Judgment and denies Plaintiffs’ Cross-Motion for Summary Judgment. A separate final order accompanies this Memorandum Opinion.

Dated: November 23, 2016


Amit P. Mehta
United States District Judge