UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

DAVE LEVINTHAL, *et al.*,	)	
Plaintiffs,	)	
v.	)	Civil Action No. 15-1624 (APM)
FEDERAL ELECTION COMMISSION,	)	
Defendant.	)	

DEFENDANT FEDERAL ELECTION COMMISSION'S
MOTION FOR SUMMARY JUDGMENT

Defendant Federal Election Commission hereby moves this Court for an order granting summary judgment to the Commission pursuant to Rule 56 of the Federal Rules of Civil Procedure and Local Rule 7(h). As discussed in the accompanying memorandum of points and authorities, the Commission has complied with its obligations under the Freedom of Information Act. There are no material facts in dispute and the Commission is entitled to judgment in its favor as a matter of law.

A proposed order and a statement of material facts not in dispute are attached to the Commission's Memorandum.

March 17, 2016
Washington, DC

Respectfully submitted,

CHANNING D. PHILLIPS, D.C. Bar #415793
United States Attorney

DANIEL F. VAN HORN, D.C. Bar #924092
Chief, Civil Division

By: /s/
WYNNE P. KELLY
Assistant United States Attorney
555 4th Street, NW
Washington, DC 20530
(202) 252-2545
wynne.kelly@usdoj.gov

Attorneys for the FEC

OF COUNSEL:

Daniel A. Petalas (D.C. Bar No. 467908)
Acting General Counsel
dpetalas@fec.gov

Lisa J. Stevenson (D.C. Bar No. 457628)
Deputy General Counsel — Law
lstevenson@fec.gov

Kevin Deeley
Acting Associate General Counsel
kdeeley@fec.gov

Erin Chlopak (D.C. Bar No. 496370)
Acting Assistant General Counsel
echlopak@fec.gov

Tanya Senanayake (D.C. Bar No. 1006218)
Attorney
tsenanayake@fec.gov

FEDERAL ELECTION COMMISSION
999 E Street NW
Washington, DC 20463
(202) 694-1650

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

DAVE LEVINTHAL, *et al.*, Plaintiffs, v. FEDERAL ELECTION COMMISSION, Defendant.	)	Civil Action No. 15-1624 (APM)

DEFENDANT FEDERAL ELECTION COMMISSION'S MEMORANDUM IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT

Plaintiffs Dave Levinthal and the Center for Public Integrity seek an order requiring the Federal Election Commission ("FEC" or "Commission") to produce, under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, documents containing analysis of vulnerabilities within the Commission's information technology systems and recommendations about addressing such vulnerabilities. FOIA plainly does not require disclosure of such privileged documents; summary judgment should be granted to the Commission.

The rate of documented cybersecurity breaches into federal government information technology systems is increasing, and such attacks are a constant threat to maintaining the integrity and confidentiality of sensitive data stored by the government. For instance, in late 2014, hackers entered unclassified networks at the White House and State Department. In July 2015, hackers accessed an internal network at the Office of Personnel Management ("OPM") and stole information concerning over 22 million people that had been stored in OPM's databases. The July 2015 cybersecurity attack followed a breach of OPM's information technology systems the month before, which resulted in the compromised data of 4.2 million federal employees. In

fact, unauthorized persons breached the FEC's own networks in May 2012. To explore further safeguards to its systems from wrongful interference by unauthorized persons and to prevent another such breach of its data, the Commission conducted a study to identify its technological vulnerabilities and to make recommendations that would allow the Commission to address any identified weaknesses.

Plaintiffs' complaint asks this Court to order that this vulnerability assessment report and associated documents be publicly disclosed. The documents, however, contain sensitive information that, if disclosed, could be used by outside persons or governments to wrongfully interfere with the Commission's information technology systems or to access the Commission's data systems to circumvent the law. They are also manifestly deliberative and predecisional. These documents are plainly privileged, and this Court should grant summary judgment to the Commission.

BACKGROUND

I. PARTIES

The Federal Election Commission ("Commission") is an independent agency of the United States government with exclusive jurisdiction over the administration, interpretation, and civil enforcement of the Federal Election Campaign Act ("FECA" or "Act"). *See generally* 52 U.S.C. §§ 30106(b)(1), 30107(a), 30109. Congress designated the Commission as the repository for reports of federal campaign finance, and required that the Commission make such reports available for public inspection and on a website. 52 U.S.C. §§ 30111(a)(4), 30112.

Congress authorized the Commission to audit committees filing disclosure reports and required that the agency determine which committees to audit by developing "threshold requirements for substantial compliance with the Act." 52 U.S.C. § 30111(b). Congress

authorized the Commission to institute investigations of possible violations of the Act, including "on the basis of information ascertained in the normal course of . . . its supervisory responsibilities." 52 U.S.C. § 30109 (a)(1)-(2). Absent a waiver, the Commission's investigations are confidential until closed and its efforts at conciliation may not be made public permanently. 52 U.S.C. § 30109(a)(4)(B)(i), (a)(12). The agency has exclusive jurisdiction to initiate civil enforcement actions in the United States district courts and is authorized to report other "apparent violations to the appropriate law enforcement authorities." 52 U.S.C. §§ 30106(b)(1), 30107(a)(6), (a)(9), 30107(e), 30109(a)(6).

According to the complaint, plaintiff Center for Public Integrity ("CPI") is a nonprofit corporation organized under 26 U.S.C. § 501(c)(3). (Compl. ¶ 5.) Plaintiff Dave Levinthal is employed by CPI. (*Id.* ¶ 4.) Plaintiffs sought the records at issue in this matter in a request submitted to the FEC pursuant to FOIA. (*Id.* ¶¶ 1, 6.)

II. THE NIST STUDY

In Fiscal Year 2014, the Commission contracted with SD Solutions, LLC ("SD Solutions") to assess the vulnerabilities of its information technology systems and to make a report of recommendations addressing any such vulnerabilities. (*See* Decl. of Alec Palmer, Chief Information Officer, the Commission, Ex. 1 to Def. St. of Mat. Facts, ¶ 7.) The Commission requested the assessment and report to inform its decision regarding whether to implement information security standards and guidelines developed by the U.S. Department of Commerce's National Institute of Standards and Technology ("NIST") for federal information systems (hereinafter referred to as the "NIST Framework"). (*Id.* ¶ 7.)[1] SD Solutions undertook an

[1] Pursuant to the Federal Information Security Management Act of 2002, 44 U.S.C. §§ 3541-49, which was in place at the time that the Commission requested the NIST Study but later replaced by the Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551,

investigation of the physical and virtual information technology assets utilized by the Commission in conjunction with the Commission's Office of the Chief Information Officer ("OCIO") and its information technology specialists. (*Id*. ¶ 8.) SD Solutions then prepared a report for the Commission that made recommendations about safeguarding the Commission's systems from wrongful interference, circumvention, or unlawful action by unauthorized persons. (*Id*. ¶ 8.) The report analyzes the Commission's technological infrastructure for vulnerabilities to external interference or harm: It describes sensitive Commission systems and recommends specific security measures to address vulnerabilities. (*Id*. ¶ 8.)

During the administrative phase of this matter, the Commission construed "the NIST Study," as requested by plaintiffs, to consist of two documents: (1) an overview memorandum prepared by the OCIO entitled "OCIO Background and Overview of the NIST Study" ("Overview Memorandum"); and (2) SD Solutions's full-length report of its recommendations, which is entitled "Gap Analysis Final Report" ("Final Report"). (*See* Decl. of Robert Kahn, Attorney, Office of General Counsel, the Commission, Ex. 2 to Def. St. of Mat. Facts, ¶ 11.) This Memorandum thus similarly refers to the Overview Memorandum, including its two appendices described below, and the Final Report collectively as the "NIST Study."

A. The Overview Memorandum

The OCIO prepared the four-page Overview Memorandum for the Commissioners at their request. (Palmer Decl. ¶ 9.) OCIO circulated the memorandum to the Commission on June 30, 2015. (*Id*. ¶ 9.) The Overview Memorandum describes specific measures, tools, and systems that the OCIO has adopted in the past to address information technology vulnerabilities and to

---

et seq., most agencies of the federal government are required to implement the NIST framework. Congress, however, exempted the Commission from this requirement. 44 U.S.C. § 3552(a) (incorporating by reference the definition of "agency" in 44 U.S.C. § 3502).

improve the Commission's ability to detect and deter cyber threats, summarizes the NIST Study, and provides information about potential implementation should the Commission adopt the recommendations in the Final Report, described below. (*Id*. ¶ 9.)

Attached as appendices to the Overview Memorandum are two documents prepared for the Commission by SD Solutions. (Palmer Decl. ¶ 10.) Appendix A, the "IT Gap Analysis – Summary," summarizes the recommendations that SD Solutions made to the Commission. (*Id*. ¶ 10.) It describes vulnerabilities in the Commission's technology infrastructure and specific measures and programs to be implemented to address the identified vulnerabilities. (*Id*. ¶ 10.) The IT Gap Analysis – Summary also provides an analysis of policies, procedures, and technical measures that could be implemented to protect Commission information systems and data. (*Id*. ¶ 10.) This document is a short-form version of the longer Final Report. (*Id*. ¶ 10.)

Appendix B to the Overview Memorandum summarizes the recommendations that SD Solutions made to the Commission in the Final Report and lists corresponding estimates of resources required to fulfill each recommendation, referred to as "Level of Effort (LOE) Estimates." (Palmer Decl. ¶ 11.) Specifically, the document states each recommendation made to the Commission, lists specific risk management and cybersecurity measures as applied to Commission systems that address the recommendation, and lists corresponding personnel and financial resources that would be required to fulfill the recommendation. (*Id*. ¶ 11.)

B. The Final Report

The second document at issue is the full version of the 30-page "Gap Analysis Final Report." (Palmer Decl. ¶ 12.) SD Solutions provided the Final Report to the OCIO on April 17, 2015, and OCIO made the Final Report available to the Commission on June 30, 2015. (*Id*. ¶ 12.) The Final Report analyzed specific technology assets, programs, and systems of the

Commission. (*Id*. ¶ 12.) The Final Report describes specific systems that SD Solutions evaluated for vulnerabilities, including the security categorization, system architecture, and technical assessment results for each system. (*Id*. ¶ 12.) With regard to system architecture, the Final Report details the physical locations, names, and attributes for Commission servers, and the applications, including anti-virus and cybersecurity software, that each server supports. (*Id*. ¶ 12.) The Final Report assesses the security of each system, listing the specific components and vulnerabilities applicable to the target system. (*Id*. ¶ 12.)

The Final Report also contains a description of the Commission's network topology, including information technology systems, servers, and applications utilized by the Commission for its enforcement, litigation, and administrative functions. (Palmer Decl. ¶ 13.) The Final Report specifically describes the Commission's Local Area Network as utilized in the headquarters office and its virtual private network used in remote locations. (*Id*. ¶ 13.) The Final Report identifies the locations, components, hostnames, and firmware that comprise this topology. (*Id*. ¶ 13.)

Finally, the Final Report contains recommendations to the Commission regarding specific security measures to address identified vulnerabilities. (Palmer Decl. ¶ 14.) These recommendations are based on identified gaps in cybersecurity specific to the Commission's information technology systems, and they incorporate security categorization and technical assessments for each system analyzed in the Final Report. (*Id*. ¶ 14.)

III. PLAINTIFFS' FOIA REQUEST

On July 6, 2015, the Commission received a FOIA request from plaintiffs 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." (Kahn Decl. ¶ 6; E-mail from Dave Levinthal, CPI, to FOIA@fec.gov (July 6, 2015), attached as Exhibit A to the Kahn Decl.) The Commission's FOIA Requestor Service Center ("FOIA Service Center") acknowledged receipt of the request the following day. (*See* Kahn Decl. ¶ 6; Email from Christopher Mealy, FEC FOIA Service Center, to Dave Levinthal, CPI (July 7, 2015), attached as Exhibit B to Kahn Decl.)

The Commission's FOIA Service Center responded to plaintiffs' FOIA request on August 18, 2015, after extending the processing period to respond to the request by an additional ten working days in accordance with 5 U.S.C. § 552(a)(6)(B)(i) and 11 C.F.R. § 4.7(c). (*See* Kahn Decl. ¶ 7; Email from Robert M. Kahn, FOIA Service Center, to Dave Levinthal, CPI (Aug.18, 2015), attached as Exhibit C to the Kahn Decl.) The FOIA Service Center's August 18 letter denied plaintiffs' request for "a copy of the 2015 National Institute of Standards and Technology report." (Kahn Decl. ¶ 7 & Exh. C.) The August 18 letter also informed plaintiffs that the second part of their FOIA request — their request for documents that mention or refer to the NIST study — was "granted in part subject to applicable FOIA exemptions." (Kahn Decl. ¶ 7 & Exh. C.)

On August 18, 2015, the same day the FOIA Service Center denied plaintiffs' FOIA request for the NIST Study, plaintiffs administratively appealed that portion of the determination to the Commission. (*See* Kahn Decl. ¶ 8; Letter from Dave Levinthal, CPI, to FOIA@fec.gov (Aug.18, 2015), attached as Exhibit D to the Kahn Decl.) Plaintiffs appealed the determination on the grounds that "[t]he study 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 & Exh. D.)

On September 15, 2015, with plaintiffs' consent, the FOIA Service Center extended the processing period to respond to the FOIA appeal by an additional ten working days to September 30, 2015, providing the Commission additional time necessary to determine whether any information in the NIST Study could be disclosed. (*See* Kahn Decl. ¶ 9; Email from Kate Higginbothom, FEC FOIA Public Liaison, to Dave Levinthal, CPI (Sept. 15, 2015), attached as Exh. E to Kahn Decl.)

By a majority vote of four or more Commissioners, the Commission voted to uphold the FOIA Service Center's determination to withhold the NIST Study and accordingly denied plaintiffs' FOIA appeal. (*See* Kahn Decl. ¶ 10.) On September 30, 2015, the Commission's FOIA Service Center so informed plaintiffs. (*See* Kahn Decl. ¶ 10; Email from Robert M. Kahn, FEC FOIA Service Center, to Dave Levinthal, CPI (Sept. 30, 2015), attached as Exh. F to Kahn Decl.)

Plaintiffs then filed a complaint for declaratory and injunctive relief in this Court on October 5, 2015. As indicated in the parties' Joint Status Report filed on January 19, 2016 (Docket No. 11), the FEC has produced over 1450 pages of non-exempt records, and non-exempt portions of records, responsive to the portion of plaintiffs' FOIA request that seeks documents that mention or refer to the NIST study, while withholding additional records that are covered by one or more FOIA exemptions. Plaintiffs do not contest the Commission's withholdings of and redactions to documents responsive to that portion of their FOIA request. (Joint Status Rpt., Jan. 19, 2016, at 1 (Docket No. 11).) The parties thus agree that the only remaining issue in this

litigation is the FEC's denial of the portion of plaintiffs' FOIA request seeking a copy of the NIST Study itself. (*Id.*)

ARGUMENT

I. STANDARD OF REVIEW

FOIA matters are typically resolved on motions for summary judgment. *Brayton v. Office of the U.S. Trade Rep.*, 641 F.3d 521, 527 (D.C. Cir. 2011). To prevail on summary judgment in a FOIA matter, "the government must demonstrate the absence of a genuine dispute regarding the adequacy of its search for or production of responsive records." *Judicial Watch, Inc. v. Dep't of the Navy*, 971 F. Supp. 2d 1, 3 (D.D.C. 2013) (citing *Nat'l Whistleblower Ctr. v. Dep't of Health & Human Servs.*, 849 F. Supp. 2d 13, 21–22 (D.D.C. 2012)).[2] If an agency withholds responsive documents, it bears the burden of demonstrating the applicability of the claimed exemptions. *ACLU v. U.S. Dep't of Def.*, 628 F.3d 612, 619 (D.C. Cir. 2011).

The government meets its burden and merits summary judgment when it submits declarations that demonstrate with adequate specificity the reason for the withholding and that "the information withheld logically falls within the claimed exemption." *ACLU*, 628 F.3d at 619; *see also Davis v. Dep't of Justice*, 970 F. Supp. 2d 10, 14 (D.D.C. 2013) (internal citation and quotation marks omitted) ("Summary judgment in a FOIA case may be based solely on information provided in an agency's supporting affidavits or declarations if they are relatively detailed and non-conclusory . . . and when they describe the documents and the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld

[2] Generally "[t]o prevail in a FOIA action, an agency must first demonstrate that it has made 'a good faith effort to conduct a search for the requested records, using methods which can be reasonably expected to produce the information requested.'" *Energy & Env't Legal Inst. v. FERC*, 72 F. Supp. 3d 241, 246 (D.D.C. 2014) (quoting *Oglesby v. Dep't of Army*, 920 F.2d 57, 68 (D.C. Cir. 1990)). In this case, however, plaintiffs do not challenge the adequacy of the Commission's search for responsive records. (Joint Status Rpt., Jan. 19, 2016, at 1.)

logically falls within the claimed exemption, and are not controverted by either contrary evidence in the record [or] by evidence of agency bad faith.").[3]

"Agency affidavits submitted in the FOIA context are . . . 'accorded a presumption of good faith.'" *Anguimate v. Dep't of Homeland Sec.*, 918 F. Supp. 2d 13, 17 (D.D.C. 2013) (quoting *SafeCard Servs., Inc. v. SEC*, 926 F.2d 1197, 1200 (D.C. Cir. 1991)). An agency's justification "for invoking a FOIA exemption is sufficient if it appears 'logical' or 'plausible.'" *Larson v. Dep't of State*, 565 F.3d 857, 862 (D.C. Cir. 2009) (quoting *Wolf v. CIA*, 473 F.3d 370, 374–75 (D.C. Cir. 2007)).

In a case brought under FOIA seeking to enjoin an agency from withholding agency records, the district court "shall determine the matter de novo." 5 U.S.C. § 552(a)(4)(B); *Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 755 (1989).

II. THE NIST STUDY IS EXEMPT FROM DISCLOSURE UNDER FOIA

A. The NIST Study is Covered by the Law Enforcement Privilege and Exempt from Disclosure Under FOIA Exemption 7(E)

The requested documents were properly withheld because they are exempt from disclosure under FOIA Exemption 7(E). FOIA Exemption 7 protects from disclosure government "records or information compiled for law enforcement purposes" when the disclosure of the records would cause "an enumerated harm." *See Strunk v. U.S. Dep't of State*,

[3] A Vaughn index is a document that lists all withheld records, the specific FOIA exemptions applicable to each, and the agency's justifications for nondisclosure. *See Vaughn v. Rosen*, 484 F.2d 820, 827 (D.C. Cir. 1973). A Vaughn index is not necessary where, as here, the agency has provided "the reviewing court a reasonable basis to evaluate the claim[s] of privilege." *Judicial Watch, Inc. v. U.S. Postal Service*, 297 F. Supp. 2d 257 (D.D.C. 2004) (internal quotation marks omitted); *see also Gallant v. NLRB*, 26 F.3d 168, 173 (D.C. Cir. 1994) (holding that "production of a Vaughn Index was not necessary given the adequacy of the government's affidavits"). This Memorandum and its supporting declarations clearly identify and describe the two documents (including the two appendices attached to one of them) at issue here, the FOIA exemptions applicable to those documents, and the Commission's clear justifications for withholding the documents based on those exemptions. *See infra* pp. 10-21.

905 F. Supp. 2d 142, 145 (D.D.C. 2012). A record is found to have been compiled for a law enforcement purpose "only if (1) it arose from an investigation related to the enforcement of federal laws or to the maintenance of national security (the nexus requirement), and (2) the nexus between the investigation and one of the agency's law enforcement duties is based on information sufficient to support at least a colorable claim of its rationality." *Id*. at 145-46 (quoting *Simon v. Dep't of Justice*, 980 F.2d 782, 783 (D.C. Cir. 1992)).

Under FOIA Exemption 7(E), law enforcement records that would "disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions" need not be released "if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E). While the first clause of the exemption categorically protects "'techniques and procedures' used in law enforcement investigations or prosecutions," the second clause "separately protects 'guidelines for law enforcement investigations or prosecutions if [their] disclosure could reasonably be expected to risk circumvention of the law.'" *Ortiz v. Dep't of Justice*, 67 F. Supp. 3d 109, 122 (D.D.C. 2014) (citing *Pub. Emps. for Envtl. Responsibility v. U.S. Section Int'l Boundary & Water Comm'n*, 839 F. Supp. 2d 304, 327 (D.D.C. 2012)). Computer records and data that, if disclosed, potentially lead to disclosure of such guidelines or otherwise allow unauthorized persons to access federal government computer systems are similarly protected under Exemption 7(E). *See, e.g.*, *Strunk*, 905 F. Supp. 2d at 149; *Miller v. U.S. Dep't of Justice*, 872 F. Supp. 2d 12, 29 (D.D.C. 2012).

The D.C. Circuit has explained that this exemption sets a "low bar for the agency to justify withholding": the agency need only provide an explanation of what procedures would be disclosed. *Blackwell v. FBI*, 646 F.3d 37, 42 (D.C. Cir. 2011) ("[E]xemption 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."); *Public Emps. for Envtl. Responsibility v. U.S. Section, Int'l Boundary and Water Comm'n,* 740 F.3d 195, 205 (D.C. Cir. 2014) (explaining that the agency must demonstrate that disclosure "might increase the risk that a law will be violated or that past violators will escape legal consequences") (internal quotation marks omitted).

The Commission is a law enforcement agency with responsibility to enforce the civil provisions of FECA. Its principal functions include providing the public with information about who is funding election campaigns for federal office, auditing some of the committees who have not substantially complied with the Act's disclosure provisions, conducting confidential investigations of possible violations of the Act, and pursuing civil enforcement actions to remedy violations of the Act. *See, e.g.*, 52 U.S.C. §§ 30106(b)(1); 30107(a)(6), (e); 30109 (a)(1)-(2), (6), (12); 30111(a)(4),(b); 30112; *see also AFL-CIO v. FEC,* 333 F.3d 168, 178-79 (D.C. Cir. 2003) (recognizing that the FEC's law enforcement functions include "compil[ing] information relating to speech or political activity *for law enforcement purposes*," and holding that a former FEC regulation that required public release of the FEC's investigatory file materials in closed administrative enforcement matters "impermissibl[y]" infringed upon the First Amendment interests of the subjects of FEC investigations (emphasis added)). The Commission's information technology systems, servers, and applications comprise a network in which the Commission stores its law enforcement information and analyses. (Palmer Decl. ¶ 16.) The components of that network store confidential law enforcement thresholds, system and application information, as well as enforcement and litigation records. These records include the thresholds for determining whether committees whose reports are deficient are referred for audits or enforcement proceedings. (*Id.* ¶ 16.) For enforcement matters, the Commission's records

include a confidential scoring system known as the Enforcement Priority System that identifies more significant cases for activation and can lead to dismissal for other matters. (*Id*. ¶ 16.) Other records include confidential, internal memoranda to the Commission regarding enforcement matters; investigative records such as subpoenas, requests for information and documents, reports of investigation, and responses to Commission-issued subpoenas and requests, some of which contain sensitive First Amendment materials; records pertaining to the negotiation of conciliation agreements and the settlement of matters under the Act; records with personally identifiable information; and other highly sensitive materials. (*Id*. ¶ 17.) Other records identify parties involved in pending administrative enforcement matters, and contain information about potential violations and settlement and collections issues for cases. (*Id*. ¶ 17.) The Commission's network allows it to fulfill its statutory obligation to administer and enforce the Act. (*Id*. ¶ 16.) The records at issue here — the components of the NIST Study — were prepared to advise the Commission about how to ensure the security of the agency's information technology infrastructure, which is necessarily related to law enforcement. *See Long v. Immigration & Customs Enf't*, No. CV 14-00109 (APM), 2015 WL 8751005, at *5 (D.D.C. Dec. 14, 2015) (finding that records about defendants' databases — which defendants used for law enforcement purposes — were compiled for law enforcement purposes because they "clearly have a rational 'nexus' to Defendants' law enforcement duties" and because of the "clear connection between the records and possible security risks or violations of law").

Indeed, the public release of this information could facilitate fraudulent access to the Commission's databases, allowing persons with malicious objectives access to the Commission's guidelines for law enforcement investigations and other material, the confidentiality of which is protected by statute, even if not explicitly "techniques and procedures for law enforcement

investigations or prosecutions." Such information is still protected under Exemption 7(E). *See, e.g.*, *Strunk*, 905 F. Supp. 2d at 149 (holding that computer codes and records were properly withheld under Exemption 7(E)); *Skinner v. U.S. Dep't of Justice*, 893 F. Supp. 2d 109, 114 (D.D.C. 2012) (finding that computer access codes associated with an agency database were properly withheld under Exemption 7(E) as law enforcement guidelines), *aff'd sub nom. Skinner v. Bureau of Alcohol, Tobacco, Firearms & Explosives*, No. 12-5319, 2013 WL 3367431 (D.C. Cir. May 31, 2013); *Miller*, 872 F. Supp. 2d at 29 (concluding that computer data because was properly withheld where disclosure could, in part, allow fraudulent access to agency's databases).

The NIST Study is an information technology vulnerability assessment, which is among the most sensitive records maintained by a federal agency. (Palmer Decl. ¶ 18.) This type of assessment contains sensitive information that, when disclosed to potential violators, can do great harm. (*Id*. ¶ 19.) The information withheld here includes sensitive information regarding the Commission's network topology, the actual functioning of the Commission's network, and the devices and applications that the Commission utilizes to detect and counter cybersecurity threats. (*Id*. ¶ 18.) This information, if publicly disclosed, could be used to gain unlawful access to the Commission's technology systems, obtain and manipulate sensitive and/or confidential data about candidates, officeholders, party committees, and others that interact with the Commission, or about pending FEC enforcement matters, and harm the Commission's ability to fulfill its civil enforcement and other statutory duties under the Act. (*Id*. ¶ 19.) Moreover, with knowledge of the Commission's internal databases, an unauthorized user could alter the disclosure data available through the Commission's public website, thereby providing false disclosure information that could adversely influence the outcome of an election. (*Id*. ¶ 20.)

The NIST Study ultimately provides a blueprint to the Commission's networks that can be used by outside persons or governments to wrongfully interfere with the Commission's information technology systems or to access the Commission's data systems to circumvent the law. (Palmer Decl. ¶ 21.)[4] As this Court has recognized, it is "clear that the potential for a cyber-attack or data breach is the kind of risk of circumvention of the law that justifies withholding under Exemption 7." *Long*, 2015 WL 8751005, at *8. Disclosing the NIST Study would thus provide a blueprint to the agency's network, allowing hackers to bypass the protection mechanisms the agency currently has in place. (Palmer Decl. ¶ 21.) A cyberattack on the Commission's systems has the potential to severely disrupt the nation's electoral processes by distorting or preventing access to campaign finance reports, or exposing sensitive information about parties regulated by the Commission. (*Id*. ¶ 24.) This threat is more prominent as the 2016 presidential primaries and general election draw near. (*Id*. ¶ 24.)

FOIA requires that "[a]ny reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt." 5 U.S.C. § 552(b). The OCIO conducted line-by-line examinations of the documents that comprise the NIST Study and, based on its expertise in information technology and with the Commission's

[4] The FEC's concerns about such interference are well founded. Among other well-documented security breaches of government information technology systems, the FEC's own networks were breached by hackers in May 2012, exposing several FEC systems and a Commissioner's user account to intrusion. (Palmer Decl. ¶ 23); *see* FEC, Audit of the Federal Election Commission's Fiscal Year 2013 Financial Statements 8-9 (Dec. 2013), http://www.fec.gov/fecig/documents/FY2013FinancialStatementAuditReport.pdf. In addition, in August 2013, the Commission became aware of an intrusion into its website, and another FEC website intrusion was detected in early fiscal year 2014. *Id.* at 9. The Office of Personnel Management ("OPM") reported a similar type of cyberattack: OPM officials reported that information taken by unauthorized persons during a November 2013 hack into OPM's computer systems provided a blueprint for a subsequent, more far-reaching cyberattack on OPM's systems in 2014. (Palmer Decl. ¶ 22); *see also, e.g.*, Evan Perez & Tom LoBianco, *U.S. Government Hacking Number Sparks Unusual Drama at Senate Briefing*, CNN (June 24, 2015, 4:57 PM), http://www.cnn.com/2015/06/24/politics/opm-hacking-senate-briefing/.

information technology assets, determined that no portion of the NIST Study could be released without "risk of circumvention of the law" because each component of the NIST Study provides a blueprint to persons who may attempt to breach the Commission's networks and thereby frustrate its law enforcement functions. (Palmer Decl. ¶ 25.) In particular, the NIST Study's descriptions of the Commission's systems, analyses of system vulnerabilities, and recommendations regarding how to best address these vulnerabilities all could assist an unauthorized person with entering the Commission's systems and causing the damage described above. (*Id.* ¶¶ 26-27.) Thus, the NIST Study is privileged in its entirety under Exemption 7(E), and no portion of the NIST Study can be segregated or disclosed. *See Henderson v. Office of the Dir. of Nat'l Intelligence*, No. CV 15-103 (RBW), 2016 WL 755608, at *6 (D.D.C. Feb. 25, 2016) (finding that defendants satisfied their segregability obligations under FOIA based, in part, on defendants' representation that release of information "that could potentially be non-exempt if released alone should nonetheless be withheld" because "potentially bad actors" could use the information to surmise the contents of withheld portions of the document); *Elec. Privacy Info. Ctr. v. Dep't of Justice Criminal Div.*, 82 F.Supp.3d 307, 322 (D.D.C. 2015) (finding that defendant provided adequate grounds for withholding documents in their entirety under Exemption 7(A) based on a detailed Vaughn Index and declarations); *see also Abdelfattah v. U.S. Immigration & Customs Enforcement*, 851 F. Supp. 2d 141, 146 (D.D.C. 2012) (finding that an affidavit attesting that records were reviewed line-by-line, a detailed Vaughn index, and declarations to explain each withholding meets agency obligation regarding segregability).

Because disclosing the NIST Study would reveal the Commission's most sensitive systems and disclose its information technology vulnerabilities, public access to this documentation could allow persons with malicious intent to gain unauthorized access to

information that could result in alteration, loss, damage, or destruction of data contained in the computer systems maintained by the Commission. The NIST Study, in its entirety, is thus plainly exempt from disclosure under FOIA Exemption 7(E). For this reason alone, summary judgment should be granted in the Commission's favor.

B. The NIST Study is Also Exempt from Disclosure as Deliberative Material Under FOIA Exemption 5

The Commission properly denied plaintiffs' FOIA request for the additional reason that the requested documents are plainly covered by the deliberative process privilege and thus exempt from disclosure under FOIA Exemption 5. Exemption 5 prevents 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 incorporates the traditional privileges that the Government could assert in civil litigation against a private litigant," including the deliberative process privilege. *Baker & Hostetler LLP v. U.S. Dep't of Commerce*, 473 F.3d 312, 321 (D.C. Cir. 2006).

The deliberative process privilege is a special privilege that recognizes the importance of internal debate in government. The privilege "protect[s] the decisionmaking processes of government agencies" and "encourage[s] the frank discussion of legal and policy issues" by ensuring that agencies are not "forced to operate in a fishbowl." *Wolfe v. Dep't of Health & Human Servs.*, 839 F.2d 768, 773 (D.C. Cir. 1988) (*en banc*) (internal quotation marks omitted). As the Supreme Court stated in *Department of Interior v. Klamath Water Users Protective Association*, "deliberative process covers 'documents reflecting advisory opinions, recommendations and deliberations comprising part of a process by which governmental decisions and policies are formulated.'" 532 U.S. 1, 8-9 (2001) (quoting *NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 150 (1975) (internal quotation marks omitted)). "The deliberative

process privilege rests on the obvious realization that officials will not communicate candidly among themselves if each remark is a potential item of discovery and front page news, and its object is to enhance 'the quality of agency decisions,' by protecting open and frank discussion among those who make them within the Government." *Id.* at 9 (quoting *Sears, Roebuck & Co.*, 421 U.S. at 151; citing *EPA v. Mink*, 410 U.S. 73, 86-87 (1973); *United States v. Weber Aircraft Corp.*, 456 U.S. 792, 802 (1984)). To qualify for the deliberative process privilege, the government must show that the documents are both "pre-decisional" and "deliberative." *Renegotiation Bd. v. Grumman Aircraft Eng'g Corp.*, 421 U.S. 168, 186 (1975). Documents are pre-decisional when they precede an agency decision and are prepared in order to assist an agency in arriving at its decision. *Judicial Watch, Inc. v. Food & Drug Admin.*, 449 F.3d 141, 151 (D.C. Cir. 2006); *see also Grand Central Partnership v. Cuomo*, 166 F.3d 473, 482 (2d Cir. 1999). Documents are deliberative when they comprise any part of the process by which government decisions are made. *Id.*; *see also Elec. Privacy Info. Ctr. v. DHS*, 384 F. Supp. 2d 100, 112-13 (D.D.C. 2005) ("[I]t is the document's role in the agency's decision-making process that controls.").

Courts have recognized a "consultant corollary" to Exemption 5, which extends the deliberative-process privilege and Exemption 5 protections to recommendations to agencies from outside contractors. *E.g.*, *Klamath Water Users Protective Ass'n*, 532 U.S. at 10 (recognizing that consultant corollary may extend to "records submitted by outside consultants [that] played essentially the same part in an agency's process of deliberation as documents prepared by agency personnel might have done"). "When an agency record is submitted by outside consultants as part of the deliberative process, and it was solicited by the agency, the D.C. Circuit has found that it is 'entirely reasonable to deem the resulting document to be an 'intra-agency'

memorandum for purposes of determining the applicability of Exemption 5.'" *Elec. Privacy Info. Ctr. v. Dep't of Homeland Securit*y, 892 F. Supp. 2d 28, 45 (D.D.C. 2012) (quoting *Nat'l Inst. of Military Justice v. Dep't of Defense*, 512 F.3d 677, 680 (D.C. Cir. 2008)). The Commission hired SD Solutions to conduct a study of its information technology systems on its behalf. Accordingly, the "consultant corollary" requires that documents prepared by SD Solutions to advise the Commission should be treated no differently than recommendations prepared by Commission employees to provide advice to the Commission.

The entire NIST Study meets both requirements of the deliberative process privilege. The documents are plainly pre-decisional: The Overview Memorandum and Final Report were both prepared prior to the Commission's decision about whether to adopt the NIST Framework; in fact, the fundamental purpose of the NIST Study was to assist the Commission in making that very decision. (Palmer Decl. ¶ 15.) The NIST Study is also deliberative and reflects the give-and-take of the consultative process: The Overview Memorandum and Final Report were circulated and made available to the Commission for the purpose of aiding the Commissioners in their deliberation about whether to adopt a NIST Framework and how best to address identified and potential cybersecurity threats. (*Id*. ¶ 15). The NIST Study itself consists of recommendations and proposals "which reflect the personal opinions of the writer[s] rather than the policy of the agency": OCIO and SD Solutions made recommendations to the Commission about safeguarding the Commission's technology systems from wrongful interference by unauthorized persons and about specific security measures to address vulnerabilities that had been identified. *See Reliant Energy Power Generation*, 520 F. Supp. 2d at 203. Neither OCIO nor SD Solutions had authority to implement any of these recommendations without the Commission's approval. (Palmer Decl. ¶ 15.)

Finally, the deliberative process privilege exempts the Commission from having to segregate and disclose any factual material contained in the documents at issue. While purely factual information is generally not exempt from disclosure pursuant to the deliberative process privilege, such material "is protected by Exemption 5 if its disclosure 'may so expose the deliberative process within an agency.'" *Petroleum Info. Corp. v. Dep't of the Interior*, 976 F.2d 1429, 1434 (1992) (quoting *Mead Data Central, Inc. v. Dep't of Air Force*, 566 F.2d 242, 256 (D.C. Cir. 1977)). An agency may also withhold factual information that is "inextricably intertwined" with deliberative material. *Mead Data Central*, 566 F.2d at 260. "[A]n agency may withhold a factual portion of a document if, in creating the document, the author undertook to separate significant facts from insignificant facts" on the grounds that the selection of facts is itself an "'exercise of judgment by an agency.'" *Reliant Energy Power Generation*, 520 F. Supp. 2d at 203 (citing *Montrose Chem. Corp. v. Train*, 491 F.2d 63, 71 (D.C. Cir. 1974)).

Line-by-line examinations of the NIST Study in an effort to identify any reasonably segregable, nonprivileged, nonexempt portions of the NIST Study that could be released confirmed that both of these bases for withholding apply to all of the factual portions of the NIST study here. (Kahn Decl. ¶ 12.) First, the Final Report's factual descriptions of the Commission's information technology systems and their vulnerabilities form the basis of the analysis in the Final Report and reflect the need for the recommended protocols that constitute the core of the NIST Study. These factual descriptions are thus "inextricably intertwined" with deliberative material. And the factual statements in the Overview Memorandum, such as descriptions of the Commission's existing systems, network infrastructure, and software; vulnerability countermeasures that OCIO has implemented; and hardware OCIO has purchased to protect the Commission's systems, are central to its analyses. (*See* Palmer Decl. ¶ 27.)

Disclosures of these factual observations would in fact release the substance of the vulnerability analysis submitted to the Commission for its consideration in determining whether to accept the NIST Study's recommendations. Therefore, the Commission had no obligation to segregate and disclose any factual material contained in the documents at issue.

Second, the OCIO selected certain vulnerabilities, countermeasures, security protocols, and recommendations to describe factually in the Overview Memorandum; this document necessarily reflects an "exercise of judgment" by describing information technology sensitivities targeted by the Commission. In *Reliant Energy Power Generation*, the defendant agency acknowledged that the factual data contained in the withheld documents was not deliberative but nevertheless argued that such data was protected because of "the manner in which staff analyzed" it. 520 F. Supp. 2d at 205-06 (explaining that investigators "ma[d]e decisions about how to look at the data, how to select portions of the data to examine, and how to interpret the data"). The court agreed. *Id.* at 206. ("[W]hile these documents are not themselves deliberative, their use by agency employees in writing the Staff Report renders them part of the deliberative process."). Here, too, the OCIO made decisions about which systems to analyze, how to define the systems, and how to interpret the vulnerability assessment data.

The entire NIST Study plainly reflects "deliberations comprising part of a process by which governmental decisions and policies are formulated." *Sears, Roebuck & Co.*, 421 U.S. at 150. The deliberative process privilege clearly applies to the documents at issue here, and provides an independent basis for the Commission's proper withholding of the entire NIST Study under FOIA Exemption 5. For this reason as well, summary judgment should be granted in the Commission's favor.

CONCLUSION

For the foregoing reasons, the Court should grant the Commission's Motion for Summary Judgment and dismiss Plaintiffs' Complaint.

March 17, 2016
Washington, DC

Respectfully submitted,

CHANNING D. PHILLIPS, D.C. Bar #415793
United States Attorney

DANIEL F. VAN HORN, D.C. Bar #924092
Chief, Civil Division

By: /s/
WYNNE P. KELLY
Assistant United States Attorney
555 4th Street, NW
Washington, DC 20530
(202) 252-2545
wynne.kelly@usdoj.gov

Attorneys for the FEC

OF COUNSEL:

Daniel A. Petalas (D.C. Bar No. 467908)
Acting General Counsel
dpetalas@fec.gov

Lisa J. Stevenson (D.C. Bar No. 457628)
Deputy General Counsel — Law
lstevenson@fec.gov

Kevin Deeley
Acting Associate General Counsel
kdeeley@fec.gov

Erin Chlopak (D.C. Bar No. 496370)
Acting Assistant General Counsel
echlopak@fec.gov

Tanya Senanayake (D.C. Bar No. 1006218)
Attorney
tsenanayake@fec.gov

FEDERAL ELECTION COMMISSION
999 E Street NW
Washington, DC 20463
(202) 694-1650