IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER, Plaintiff, v. UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Defendant.	Case No. 1:17-cv-2047 JEB

MEMORANDUM IN SUPPORT OF
DEFENDANT'S MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTRODUCTION

This action pertains to a request submitted to the Department of Homeland Security ("DHS") under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, seeking records relating, *inter alia*, to DHS's research and analysis of interference with the 2016 federal elections by or at the direction of the Russian Government. As explained below, after reviewing the records provided, the parties have narrowed the issues in dispute to twelve documents withheld in full under FOIA's Exemptions 5 and 7E. The declaration of James V.M.L. Holzer ("Holzer Decl."), the Deputy Chief FOIA Officer for DHS's Privacy Office, establishes that DHS properly withheld the documents in full. Accordingly, the Court should grant DHS's motion for summary judgment.

BACKGROUND

On March 31, 2017, the Electronic Privacy Information Center ("EPIC") submitted a FOIA request to DHS. Compl. ¶ 19, ECF No. 1. The request sought two categories of records:

> A. Any document, record, memo, correspondence, or other communications or any portion of any communication of the Department of Homeland Security that refers to or relates to the following:
>
> 1. Research, integration, and analysis activities of the Department relating to interference with the elections for Federal office held in 2016 by at the direction of the Russian Government, as announced in a joint statement with the Office of National Intelligence on October 7, 2016, and December 29, 2016.[1]
>
> 2. Dissemination by the Department of Information regarding interference with the elections for Federal office held in 2016 by or at the direction of

[1] The October 7th joint statement is available at https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national, and the December 29th joint statement is available at https://www.dhs.gov/news/2016/12/29/joint-dhs-odni-fbi-statement-russian-malicious-cyber-activity.

the Russian Government, as announced in a joint statement with the Office of the Director of National Intelligence on October 7, 2016, and December 29, 2016.

3. Research into cyber compromises of emails of the United States persons and institutions by at the direction of the Russian Government to interfere with the elections for Federal office held in 2016.

4. Integration, analysis, and dissemination of the Joint Analysis Report detailing the tools and infrastructure associated with the elections for Federal Office held in 2016 issued by the Secretary of Homeland Security and Director of the Federal Bureau of Investigation on December 29, 2016.

B. Any and all information prepared for and/or transmitted to the House of Representative pursuant to House Resolution 235.

Id.. ¶ 19. The request was referred to DHS's National Protection and Programs Directorate ("NPPD"), which is now DHS Cybersecurity and Infrastructure Security Agency ("CISA"). *Id.* ¶ 20.

On October 4, 2017, EPIC filed this action seeking to compel production. *See generally* Compl. The parties conferred regarding the proposed search and processing schedule. Proposed Briefing Schedule, ECF No. 8. After CISA completed its processing, the parties conferred in an effort to narrow the scope of issues in dispute. As part of this process, CISA provided EPIC with additional information about the records withheld-in-full and also conducted a supplemental search. *See* Joint Status Reports, ECF Nos. 12 – 17, 19 and 21.

After reviewing DHS's production and the information provided by CISA about the withheld-in-full documents, EPIC requested that CISA reprocess 16 documents (94 pages). *See* Joint Status Report ¶ 7, ECF No. 22. The documents fell into four categories: (1) documents concerning contacts between DHS and State Election Officials; (2) Election Task Force meeting minutes; (3) documents about risk characterizations and analysis on inference in election

infrastructure[2] and (4) incident reports about the vulnerabilities in election systems. *Id.* ¶ 5. In an effort to continue the parties' efforts to narrow the issues in dispute, CISA agreed to reprocess the 16 documents (94 pages) identified by EPIC. *See Id.* ¶ 8.

On February 14, 2020, DHS sent a letter informing EPIC that it had reprocessed the 16 documents identified by EPIC. Joint Status Report ¶ 5, ECF No. 23. DHS released three pages in full and withheld five pages in part and 80 pages in full pursuant to Exemptions 5, 6 and/or 7(E), although the letter inadvertently stated that four pages were released in full and four pages released in part. *Id.* Two of the documents withheld in full (NPPD 001115 − NPPD 001119 and NPPD 001864 − NPPD 001875) are duplicates. *Id.* at 2 n.2. In its letter, DHS explained that one document (NPPD 000956−NPPD 000961) required further consultation with another agency. *Id.* On February 28, 2020, DHS completed its consultation and released this six page document in full. *Id.* ¶ 6.

Based on its review, EPIC informed DHS that it has narrowed its challenges to the Exemption 5 and 7(E) withholdings, and the issue of segregability, with respect to twelve of the reprocessed documents, which were withheld in full. *Id.* ¶ 7. EPIC is not challenging any other withholdings or the adequacy of CISA's searches. *Id.*

STANDARD OF REVIEW

The FOIA represents a balance struck by Congress "between the right of the public to know and the need of the Government to keep information in confidence." *John Doe Agency v. John Doe Corp*., 493 U.S. 146, 152 (1989) (citation omitted). Congress recognized "that

[2] The third category of documents that Plaintiff identified included two documents that have been released and thus are no longer the subject of Plaintiff's challenge. The remaining document in this category is a document entitled "Election Infrastructure Cyber Risk Characterization," and DHS is referring to this document by its title *infra*.

legitimate governmental and private interests could be harmed by release of certain types of information and provided nine specific exemptions under which disclosure could be refused." *FBI v. Abramson*, 456 U.S. 615, 621 (1982). While these exemptions are to be "narrowly construed," *id.* at 630, courts must not fail to give them "meaningful reach and application." *John Doe Agency*, 493 U.S. at 152; *accord Food Marketing Inst. v. Argus Leader Media*, 139 S.Ct. 2356, 2366 (2019).

A court may award summary judgment to an agency with regard to the exemptions on the basis of information provided in affidavits or declarations which "describe the documents and the justifications for nondisclosure with reasonably specific detail, demonstrate that the information withheld logically falls within the claimed exemption[s], 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).

Given this standard of review, the discussion below and attached declaration demonstrate that the information withheld is protected by one or more of the FOIA exemptions.

ARGUMENT

I. DHS Properly Withheld Information Pursuant to Exemption 5's Deliberative Process Privilege.

Exemption 5 protects from disclosure "inter-agency or intra-agency memorandums or letters which would not be available by law to a party . . . in litigation with the agency." 5 U.S.C. § 552(b)(5). Records are exempt from disclosure if they would be "normally privileged in the civil discovery context." *NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 149 (1975). Thus, Exemption 5 incorporates the privileges that are available to an agency in civil litigation, including the deliberative process privilege. *See id*. at 148−50.

The deliberative process privilege is a "long-recognized privilege" intended to "prevent injury to the quality of agency decisions" by permitting "the withholding of all papers which reflect the agency's group thinking in the process of working out its policy." *Id.* at 151, 152−53; *accord Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 866 (D.C. Cir. 1980) (the purpose of the deliberative process privilege is to protect "the give-and-take of the consultative process"). "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 discussions among those who make them within the Government." *Dep't of Interior v. Klamath Water Users Protective Ass'n*, 532 U.S. 1, 8-9 (2001) (citations omitted). In addition, the privilege seeks to protect against premature disclosure of proposed policies before they are actually adopted, and to prevent public confusion that might result from disclosure of the reasons and rationales that were not in fact ultimately the grounds for the agency's action. *See Russell v. Dep't of the Air Force*, 682 F.2d 1045, 1048 (D.C. Cir. 1982). This privilege allows the government to "withhold documents and other material that would reveal 'advisory opinions, recommendations and deliberations comprising part of a process by which government decisions and policies are formulated." *In re Sealed Case*, 121 F.3d 729, 737 (D.C. Cir. 1997) (citing cases).

To qualify for the deliberative process privilege, the materials in question must be "both 'predecisional' and 'deliberative.'" *Pub. Citizen, Inc. v. Office of Mgmt. & Budget*, 598 F.3d 865, 874 (D.C. Cir. 2010) (quoting *Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d at 866). "To establish that a document is predecisional, the agency need not point to an agency final decision, but merely establish what deliberative process is involved, and the role the

documents played in the process." *Judicial Watch v. Export-Import Bank*, 108 F. Supp. 2d 19, 35 (D.D.C. 2000). A document is "deliberative" if "it reflects the give-and-take of the consultative process." *Coastal States Gas Corp.*, 617 F.2d at 866.

All twelve of the documents at issue were withheld in full pursuant to the deliberative process privilege. The documents fall into four categories: (1) summaries of meetings between DHS and State election officials; (2) Election Task Force meeting minutes; (3) a report entitled "Election Infrastructure Cyber Risk Characterization;" and (4) incident reports. Declaration of James Holzer ("Holzer Decl.") ¶¶ 19 – 22. As explained below, the withholdings in each category meet the requirements for the deliberative process privilege because they are both predecisional and deliberative. *Id.* ¶¶ 16−22. CISA's senior leaders are responsible for carrying out CISA's mission, which includes identifying and addressing the most significant risks to critical infrastructure. *Id.* ¶ 17. The documents were provided to brief CISA's senior official aid those officials in making decisions regarding the assessment and management of risks to critical infrastructure. These documents are therefore pre-decisional, inasmuch as they precede the decision being advised on, and do not embody final agency action. *Id.* The documents are further deliberative in that they reflect the drafters' preliminary view of the facts and their relevancy and their thoughts, opinions, and recommendations. *Id.* 17. Moreover, as established in Holzer Declaration, the DHS "reasonably foresees that disclosure [of these documents] would harm an interest protected by [Exemption 5]." 5 U.S.C. § 552(a)(8)(A)(i)(1).[3]

[3] Congress made clear that this provision simply codified existing government policy that had been in place for the better part of a decade. H.R. Rep. No. 114-391 (2016), at 9 (noting that the policy was established by executive memoranda in 2009); S. Rep. 114-4 (2015), at 323 (same).

Contacts between the DHS and State Election Officials: The five documents in this category are DHS employees' frank summaries of meetings with State election infrastructure.[4] Holzer Decl. ¶ 19. They contain recommendations, emphasized points, and key areas of concern. *Id.* The documents further contain staff assessments of the meetings and engagements with certain State officials and agency staff's then-current tracking and understanding of the status of vulnerabilities in certain States' election infrastructure, along with recommendations for future action as a result of those assessments and understanding. *Id.* The assessments are not final and reflect substantial uncertainty. *Id.* The documents were used only internally within DHS and were provided to agency leadership on an on-going basis to help leadership track the current status of staff engagement with State officials and to aid leadership in making decisions regarding time and resources priorities to meet emerging needs related to the agency's election infrastructure security activities. *Id.* Release of the summaries of the contacts with State Election Officials would foreseeably harm the agency by inhibiting agency staff's ability to communicate frank, current, non-final assessments to agency leadership, which would harm agency leadership decision-making by depriving them of developing information. *Id.* ¶ 19. Further, release of non-final information would give the public an erroneous understanding of the basis for agency decisions. *Id.*

Election Task Force meeting minutes: The two documents in this category are also both predecisional and deliberative.[5] Id. ¶ 20. The Task Force advised and provided information to the Secretary of Homeland Security, the Under Secretary of NPPD, and other agency leadership

[4] *See* NPPD 000351 − 000361; NPPD 000401 − 000410; NPPD 000419; NPPD 000944; NPPD 000967.

[5] *See* NPPD 000394 – 000400; NPPD 000505 – 000507.

regarding election security. *Id.* The Task Force was a temporary mechanism and was disbanded when the Under Secretary of NPPD determined that its functions could be operated within NPPD offices. *Id.* The minutes, shared only with the agency, contain reports, status updates and assessments from individual Task Force members in furtherance of the Task Force's goal of assessing risk to the election infrastructure. *Id.* The Task Force meeting minutes also reflect potential recommendations that the Task Force would make to agency leadership to allow the leadership to make decisions regarding the planning, resourcing, and prioritization of DHS's election infrastructure security efforts. *Id*. Disclosure of the information would have a chilling effect on the deliberative discussions of agency task forces, which study particular issues and provide recommendations to agency leadership. *Id*. Chilling this communication between agency employees and between agency staff and leadership would undermine the agency's ability to perform its duties. *Id*. CISA depends on the ability of its employees to offer candid ideas and opinions to agency decision-makers and to each other without the fear of public exposure; to curtail this process would be detrimental to CISA and all government entities. *Id*.

Election Infrastructure Cyber Risk Characterization Report: The document in the third category is a report entitled "Election Infrastructure Cyber Risk Characterization."[6] *Id.* ¶ 21. It was prepared by the Office of Cyber and Infrastructure Analysis, a subcomponent of CISA, for wider Departmental leadership consideration and to aid in decisions regarding areas where the agency could best help mitigate risks to election systems. *Id*. The document was prepared for internal purposes only and contains select, non-final, in-process assessments and characterization of election infrastructure vulnerabilities. *Id*. The office provided the assessments and

[6] *See* NPPD 000926 – 000942.

characterization to support DHS's planning to enhance security of election infrastructure and to aid decisions regarding areas where the agency could best help mitigate risk to election systems, and selected the assessments and characterizations that in the office's judgment were most relevant to leadership planning at that time. Id. Disclosure of the Election Infrastructure Cyber Risk Characterization would also foreseeability harm the deliberative process. These assessments were provided to help develop Departmental plans regarding ways to enhance election infrastructure security. *Id.* ¶ 21. Disclosure of the information would foreseeably harm the agency's ability to assemble and communicate such information for leadership planning. *Id.* Further, disclosing non-final assessments of vulnerabilities could mislead the public as to the reasons and basis for later agency actions and final assessment of facts. *Id.*

Incident Reports: The four documents in the last category are incident reports about vulnerabilities in election systems.[7] *Id.* ¶ 22. They reflect non-final assessments of election infrastructure defense, agency staff analysis and recommendations, and coordination plans. *Id.* The reports contain unverified, preliminary information, and timelines of on-going agency staff engagements and discussions, which were documented for and provided to agency leadership's situational awareness and oversight to aid in planning of election infrastructure security efforts. *Id.* The reports also contained preliminary findings provided to another federal agency along with recommendations for that agency's consideration. *Id.*

Accordingly, the DHS has met its burden to demonstrate that there is information within these records that is both pre-decisional and deliberative, and therefore, exempt from disclosure.

Accordingly, the DHS properly withheld the documents at issue pursuant to Exemption 5.

[7] *See* NPPD 000962; NPPD 000963 – 000966; NPPD 001151 – 001119; NPPD 001095 – 001106.

II. DHS Properly Withheld Information Pursuant to Exemption 7(E).

Exemption 7(E) protects from disclosure "records or information compiled for law enforcement purposes" that "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). DHS withheld in full eight records at issue pursuant to this exemption: three summaries of meetings between DHS and State election officials (NPPD 000419; NPPD 000944; NPPD 000967); the Election Infrastructure Cyber Risk Characterization Report (NPPD 000926 – 000942) and four incident reports (NPPD 000962; NPPD 000963 – 000966; NPPD 001115 – 001119; NPPD 001095 – 001106). Holzer Decl. ¶ 23.

To fall within this exemption, the documents must first meet the threshold requirement that records were "compiled for law enforcement purposes." 5 U.S.C. § 552(b)(7). "[T]he term 'compiled' in Exemption 7 requires the document to be created, gathered, or used by an agency for law enforcement purposes at some time before the agency invokes the exemption." *Pub. Empls. for Envtl. Responsibility v. U.S. Section, Int'll Boundary and Water Commission*, 740 F.3d 195, 203 (D.C. Cir. 2014) ("*PEER*"). As Justice Alito explained in his concurrence in *Milner*, "[t] ordinary understanding of law enforcement includes not just investigation and prosecution of offenses that have already been committed." *Milner v. Dep't of Navy*, 562 U.S. 562, 583 (2011) (Alito, J., concurring.) It includes "proactive steps designed to prevent criminal activity and to maintain national security." *Id.* Accordingly, courts have found that compiled for law enforcement purposes include emergency action plans describing the security precautions that law enforcement personnel should implement around dams during emergencies, *PEER*, 740 F.3d at 202, a document describing the protocol for shutting down wireless networks during

critical emergencies, *Electronic Privacy Information Center v. U.S. Dep't of Homeland Security*, 777 F.3d 518, 522 (D.C. Cir. 2015), and inundation maps used to an agency to maintain law and order within reclamation projects and lands, *Living Rivers, Inc. v. U.S. Bureau of Reclamation*, 272 F. Supp. 2d 1313 (D. Utah 2003).

The records withheld by DHS under Exemption 7(E) meet this threshold. The documents were compiled for law enforcement purposes relevant to the CISA's effort to secure the Nation's election system infrastructure. Holzer Decl. ¶ 24. The documents discuss potential vulnerabilities and steps to safeguard election systems from interference and/or incidents in which there may have been tampering or interference with the election system. The Secretary of Homeland Security's responsibilities relating to infrastructure security include accessing, receiving, and analyzing law enforcement information in order to identify and assess the nature and scope of terrorist threats. *See* 6 U.S.C. § 652(e)(1)(A). DHS's responsibilities further include making recommendations on protective measures for critical infrastructure in coordination with other Federal agencies and with State, local, tribal, and territorial government agencies. *See Id.* § 652(e)(1)(C). As a component of DHS, CISA has responsibility and authority for overseeing critical infrastructure protection, including election infrastructure. Holzer Decl. ¶ 24. The documents CISA has protected pursuant to FOIA Exemption 7(E) were compiled pursuant to these responsibilities and used for the purposes of assessing threats to election system infrastructure and making recommendations for the protection thereof. *Id.* These documents contain information about coordination with other Federal law enforcement agencies and State government representatives responsible for election infrastructure security. *Id.*

The records also "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 requirement that "disclosure could reasonably be expected to risk circumvention of the law" presents a "low bar." *See PEER*, 740 F.3d at 204−05 & n.4 (saying that "it is not clear" that the issue of whether an agency needs to show that disclosure of a technique or procedure could reasonably be expected to risk circumvention of the law "matters much in practice" given the "low bar" for the circumvention requirement). "[T]he text of exemption 7(E) is much broader" than other exemptions that "set a high standard." *Mayer Brown LLP v. IRS*, 562 F.3d 1190, 1194 (D.C. Cir. 2009). "Rather 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.* (citation omitted). Therefore, Exemption 7(E) "exempts from disclosure information that could increase the risks that a law will be violated or that past violators will escape legal consequences." *Id*. at 1193

Here, release of information describing the steps CISA takes to assess and mitigate risks to election systems would divulge nonpublic procedures to safeguard election system infrastructure and to detect possible interference. Holzer Decl. ¶ 25. Were the public made aware of the procedures CISA uses to assess and respond to cybersecurity incidents on or vulnerabilities in states' election systems, it could allow bad actors who intend to disrupt the Nation's election infrastructure to evade CISA's detection techniques and circumvent its mitigation procedures, which would put states' election systems at greater risk. *Id.*

Because CISA's election system security efforts include assessing where risks are highest and which states may be subject to greater vulnerabilities, disclosure of CISA's assessments would enable bad actors to target certain states or areas, significantly increasing their risks. Moreover, because some of the documents contain discussions of specific incidents, release of the information would alert those who attempted to compromise the election infrastructure of the degree to which their actions were detected. *Id.* This may encourage those actors to either try the same measures again if they perceive they were not fully detected or to try other means that they believe would more effectively evade detection. *Id.*

For example, the Election Infrastructure Cyber Risk Characterization Report (NPPD 000926 – 000942) contains detailed information concerning assessment of states' election infrastructure vulnerabilities, risks of cyber intrusion and mitigation possibilities. Holzer Decl. ¶ 27. The report describes in detail nonpublic techniques and procedures that the agency uses to make such assessment. *Id.* Release of this information would allowing targeting of states perceived to have higher risk factors or provide models for disrupting elections systems. Similarly, the incident reports of tests of state election infrastructure (e.g. NPPD 000966) contain reports of tests of state election infrastructure and vulnerability assessments, which were not made public. Holzer Decl. ¶ 28. Disclosure of the test techniques and results would reveal the technique and procedures used to access and respond to states' infrastructure vulnerabilities. *Id.* Disclosure of such technique would risk rendering the techniques and procedures ineffective. *Id.* Likewise, charts of contact between NPPD and State Election Officials contain nonpublic techniques and procedures CISA uses to assess and address risks to vulnerabilities in states' election infrastructure. Holzer Decl. ¶ 29. Release of this information would put such

techniques and procedures at risk of being undermined or rendered ineffective and allow targeting of states with perceived greater risk factors. *Id.*

Accordingly, DHS properly withheld documents pursuant to Exemption 7(E).

III. DHS Released All Reasonably Segregable Information.

The 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 under this subsection." 5 U.S.C. § 552(b). DHS has met that burden here because it conducted a line-by-line review of each CISA record to achieve maximum disclosure consistent with the access provisions of the FOIA. Holzer Decl. ¶ 30. Where, as here, the pages were withheld in full, all information was either fully covered by one or more FOIA exemptions or any non-exempt information was so intertwined with exempt material that no information could be reasonably segregated for release. *Id. See Johnson v. Exec. Office for U.S. Attorneys*, 310 F.3d 771, 776-77 (D.C. Cir. 2002) (agency demonstrated there was no reasonably segregable non-exempt information where it submitted affidavit showing that agency had conducted line-by-line review of each document withheld in full). Therefore, DHS is entitled to summary judgment.

CONCLUSION

For the foregoing reasons, the Court should grant DHS's summary judgment on all of Plaintiff's claims.

Respectfully submitted,

ETHAN P. DAVIS
Principal Deputy Assistant Attorney General

MARCIA BERMAN
Assistant Branch Director

/s/ Marcia K. Sowles
MARCIA K. SOWLES (DC Bar 36944)

Senior Trial Attorney
U.S. Department of Justice
Civil Division, Federal Programs Branch
1100 L Street, N.W.
Washington, D.C. 20530
Telephone: (202) 524-4960
Fax: (202) 616-8470
E-mail: marcia.sowles@usdoj.gov

Counsel for Defendant