IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER, Plaintiff, v. UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Defendant.	Civ. Action No. 17-2047 (JEB)

MEMORANDUM OF POINTS AND AUTHORITIES
IN SUPPORT OF PLAINTIFF'S COMBINED OPOSITION TO
DEFENDANT'S MOTION FOR PARTIAL SUMMARY JUDGMENT
AND CROSS-MOTION FOR PARTIAL SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

PRELIMINARY STATEMENT

This case arises from a series of Freedom of Information Act ("FOIA") requests filed by the Electronic Privacy Information Center ("EPIC") seeking disclosure of records concerning the United States Department of Homeland Security's ("DHS's") assessment of cybersecurity vulnerabilities and breaches of election infrastructure during 2016. Since EPIC filed suit in 2017, the DHS has disclosed several hundred pages of responsive records and the parties have significantly narrowed the issues in dispute. The remaining records in dispute include minutes of the Election Cybersecurity Taskforce, summaries of communications between DHS and state election officials, the agency's September 2016 assessment of cybersecurity risks to election infrastructure, and incident reports concerning significant election vulnerabilities uncovered in 2016. The DHS is withholding these twelve records in full, and the agency asserts that they are exempt from disclosure under the FOIA. These documents contain factual information about vulnerabilities in our election systems in 2016, and the DHS's responses to those vulnerabilities, as well as the agency's formal assessments about election vulnerabilities in the lead up to the 2016 Election. The United States cannot afford to repeat past mistakes and leave our election systems vulnerable. It is essential that the public be given full access to the facts and assessments that provide the basis for oversight and security of our election systems.

EPIC is entitled to summary judgment on its FOIA claims because the agency has not met its burden to demonstrate that the records at issue are protected under the deliberative process privilege or that the records would disclose techniques and procedures for law enforcement investigations and prosecutions.

The 2020 election is fast approaching, and the prompt disclosure of these records is clearly in the public interest. The Court should grant EPIC's Cross Motion for Partial Summary

Judgment, deny the DOJ's Motion for Partial Summary Judgment, and order the agency to release the withheld information.

BACKGROUND

I. The DHS's Role in Securing Election Infrastructure

Despite the agency's original focus on responding to and preventing terrorist threats, the Department of Homeland Security has played a key role in coordinating a completely unrelated set of government activities: assessments of, responses to, and education regarding cybersecurity vulnerabilities. In 2008, President Bush established a Comprehensive National Cybersecurity Initiative and tasked the DHS with "defending, protecting and reducing vulnerabilities on Federal Executive Branch networks and systems." The White House, *The Comprehensive National Cybersecurity Initiative* (2009).[1] It was later revealed, through EPIC's FOIA litigation, that President Bush had established a command structure for cybersecurity policy through a National Security Presidential Directive in 2008. EPIC, *EPIC v. NSA: EPIC Obtains Presidential Directive for Cybersecurity* (2014).[2] Then, in 2013, President Obama issued the Presidential Policy Directive 21—Critical Infrastructure Security and Resilience (PPD-21), which underscored the DHS's responsibility to strengthen and secure critical infrastructure against physical and cyber threats. Directive on Critical Infrastructure Security and Resilience, 2013 Daily Comp. Pres. Doc. (Feb. 12, 2013).[3] PPD-21 directed the Secretary of Homeland Security to provide "strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure." *Id.* at 2.

---

[1] https://www.govinfo.gov/content/pkg/DCPD-201300092/pdf/DCPD-201300092.pdf.
[2] https://epic.org/2014/06/epic-v-nsa-epic-obtains-presid.html.
[3] https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Up until 2018, the DHS's National Protection and Programs Directorate ("NPPD") oversaw the protection of critical infrastructure, including protection against cyber threats. Dep't of Homeland Sec., *NPPD at a Glance* (2018).[4] The NPPD was established in 2007 and focused on the agency's risk-reduction mission to protect critical systems. *See* Dep't of Homeland Sec., National Infrastructure Protection Plan: 2007/2008 Update 35 (2008).[5] After the issuance of PPD-21, NPPD focused, in particular, on identifying and assessing cybersecurity vulnerabilities to critical infrastructure, as well as provide recommendation and assistance in developing protective measures against cybersecurity vulnerabilities. *Id.* Election infrastructure was a subsector of the government facilities sector and part of NPPD's mission in protecting critical infrastructure. Office of Inspector General, Dep't of Homeland Sec., *Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure* 5, OIG-19-24 (Feb. 28, 2019) [hereinafter DHS OIG Report].[6] The NPPD developed partnerships on the federal, state, and local level with critical infrastructure owners and operators. *Id.* The DHS also tracks and disseminates cyber threat information concerning many types of critical infrastructure, including threats to election systems in the lead up to the 2016 election. *See* Ex. 1, Dep't of Homeland Sec. & Fed. Bureau of Investigation, Threats to Federal, State, and Local Government Systems, JAR-16-20223 (Oct. 14, 2016).

On January 6, 2017, then DHS Secretary Jeh Johnson announced the designation of election infrastructure as a subsector of the Government's critical infrastructure. Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure

[4] https://www.cisa.gov/sites/default/files/publications/nppd-at-a-glance-bifold-02132018-508.pdf.
[5] https://www.dhs.gov/xlibrary/assets/nipp_update_2007_2008.pdf.
[6] https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-24-Feb19.pdf.

Subsector (Jan. 6, 2017).[7] Former DHS Secretary Johnson has since stated that he made the designation after "concerns about the possibility of a cyberattack around our national election grew" following the events of 2016. *Russian Interference in the 2016 U.S. Elections: Hearing Before H. Permanent Select Comm. on Intelligence*, 115th Cong. (2017) (written opening statement of Jeh Johnson, former Secretary, Department of Homeland Security) [hereinafter Jeh Johnson HPSCI testimony].[8] Because elections are governed and administered by state and local election officials, election systems are managed at the state level. With the designation of election systems as critical infrastructure, the NPPD formalized the prioritization of voluntary cybersecurity assistance to state and local election infrastructure. *Cybersecurity of Voting Machines: Hearing Before the Subcomm. on Info Technology & Intergovernmental Affairs of the H. Comm. on Oversight and Gov't Reform*, 115th Cong. (2017) (written testimony of NPPD Senior Official performing the duties of Under Sec. Christopher Krebs).[9] Since the 2016 Election, NPPD officials and state election officials "have met regularly to share cybersecurity risk information and to determine effective means of assistance." *Id.*

In response to election interference in 2016 and anticipating similar threats in 2018, the NPPD created an Election Security Task Force comprised of stakeholders across the DHS. The DHS Election Security Task Force "serve[d] to provide actionable information to assist states in strengthening their election infrastructure against cyber threats." *Id.* Earlier this year, DHS disbanded the Election Security Task Force and its members were reassigned to different roles in

[7] https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.
[8] https://docs.house.gov/meetings/IG/IG00/20170621/106152/HHRG-115-IG00-Wstate-JohnsonJ-20170621.pdf.
[9] https://www.dhs.gov/news/2017/11/29/written-testimony-nppd-house-oversight-and-government-reform-subcommittees.

the agency. Erin Banco & Betsy Swan, *Trump's DHS Gusts Task Forces Protecting Elections From Foreign Meddling*, Daily Beast (Feb. 14, 2020).[10]

In 2018, President Trump signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018, which established the Cybersecurity and Infrastructure Security Agency ("CISA"). *See* 6 U.S.C. §§ 651–74. CISA replaced and integrated the resources and responsibilities of the NPPD and became its own operational agency, which meant having greater independence and power than NPPD. *Id.* CISA states that its mission is to "build[] the national capacity to defend against cyberattacks" by working with partners and the federal government to protect election systems. Cybersecurity and Infrastructure Sec. Agency, *About CISA* (2020).[11] CISA provides "voluntary assistance and support" to state and local election officials "in the form of advice, intelligence, technical support, and incident response." Cybersecurity and Infrastructure Sec. Agency, *#Protect2020 Strategic Plan* 4 (Feb. 2020).[12] Some key areas of CISA's services include: cybersecurity advisory and protective security advisory services, cybersecurity assessments, detection and prevention, information sharing awareness, incident response, and training and career development. Dep't of Homeland Sec., *Election Security: Our Election Services* (June 9, 2020).[13]

II. The Detection and Reporting of Russian Interference in the 2016 Election

The U.S. Intelligence Community conducted an investigation in late 2016 and concluded that Russia carried out a multi-pronged campaign to interfere in U.S. Presidential Election and to

[10] https://www.thedailybeast.com/trumps-dhs-guts-task-forces-protecting-elections-from-foreign-meddling.
[11] https://www.cisa.gov/about-cisa.
[12] https://www.cisa.gov/sites/default/files/publications/ESI%20Strategic%20Plan_FINAL%202.7.20%20508.pdf.
[13] https://www.dhs.gov/topic/election-security.

"undermine public faith in the US democratic process." Office of the Dir. of Nat'l Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections* ii (2017).[14] In particular, Russian affiliated groups probed state election systems for vulnerabilities, hacked and leaked documents from Democratic committees and campaigns,[15] attempted to infiltrate systems managed by Republican campaigns, including Senator Marco Rubio and the Republican National Committee, targeted voting blocks and institutions, and spread disinformation on social media. Abigail Abrams, *Here's What We Know So Far About Russia's 2016 Meddling*, Time (Apr. 18, 2019).[16] In the three years since the Intelligence Community released its report detailing this election interference campaign, many of the details of the hacking and disinformation operations have been made public through agency memorandums, court documents, testimony, and news reports.

The DHS has played a key role in the federal government's tracking, assessment, and responses to election interference because the DHS is responsible for coordinating cybersecurity policy for government systems. On December 29, 2016, DHS worked with the Federal Bureau of Investigation published the first public report on the interference—the "Joint Analysis Report" ("JAR"). Dep't of Homeland Sec. & Fed. Bureau of Investigation, *GRIZZLY STEPPE – Russian Malicious Cyber Activity* (2016).[17] The JAR highlighted and explained some of the interference techniques used by the Russians and some of the techniques used by the Government in defense of voting systems. Most significantly, the JAR formally tied the attack to Russian intelligence

[14] https://www.dni.gov/files/documents/ICA_2017_01.pdf.
[15] Russia-affiliated groups hacked the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee.
[16] https://time.com/5565991/russia-influence-2016-election/.
[17] https://www.us-cert.gov/sites/default/files/publications/JAR_1620296A_GRIZZLY%20STEPPE-2016-1229.pdf.

services. Unlike earlier JARs, which did "not attribute[] malicious cyber activity to specific countries or threat actors," the 2016 JAR immediately identified "Russian civilian and military intelligence Services (RIS)" as the source of the attack. *Id.* at 1. The DHS explained that Russian actors "compromise[d] and exploit[ed] networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities." *Id.*

On June 21, 2017, nearly eight months after election day, in an open hearing before the Senate Select Committee on Intelligence, National Protection and Programs Directorate's ("NPPD") Acting Deputy Under Secretary for Cybersecurity and Communications Jeanette Manfra confirmed that "election-related systems in 21 states were targeted" by Russian cyber actors during the 2016 Election. *Russian Interference in the 2016 U.S. Elections: Hearing Before S. Select Comm. on Intelligence*, 115th Cong. (2017) (testimony of Jeanette Manfra, Acting Deputy Under Secretary, Department of Homeland Security).[18] NPPD found that nearly *half* of the states in the U.S. were targeted by Russian activities. Hackers accessed two states' election systems and downloaded hundreds of thousands of voter records, including sensitive personal information. *See* Dustin Volz & Jim Finkle, *FBI Detects Breaches Against Two State Voter Systems*, Reuters (Aug. 29, 2016).[19]

Former DHS Secretary Johnson emphasized in written testimony to the House Select Committee on Intelligence, on June 21, 2017, that this "very troubling experience highlights cyber vulnerabilities in our political process, and in our election infrastructure itself. With the experience fresh in our minds and clear in our rear-view mirror, we must resolve to further

[18] https://www.intelligence.senate.gov/hearings/open-hearing-russian-interference-2016-us-elections.
[19] https://www.reuters.com/article/us-usa-election-cybersecurity/fbi-detects-breaches-against-two-state-voter-systems-idUSKCN1141L4.

strengthen our cybersecurity generally, and the cybersecurity around our political/election process specifically." Jeh Johnson HPSCI testimony, *supra*, at 6. Secretary Johnson came forward with information about the interference after "recogniz[ing] we had an overriding responsibility to inform the public that a powerful foreign state actor had covertly intervened in our democracy." *Id.*

Since the publication of the JAR and the critical infrastructure designation, DHS has continued to assess the extent of Russian interference and has adopted a mandate to protect the cybersecurity of election systems.

In a September 12, 2019, unclassified DHS assessment, the agency stated that "Russian influence actors almost certainly will continue to target U.S. audiences with influence activities that seek to advance Russian interests, and probably view the 2020 presidential election as a key opportunity to do so." Martin de Bourmont & Jana Winter, *DHS Warns of Russian Interference Plans in 2020 Elections, as Washington Focuses on Ukraine*, Yahoo News (Oct. 24, 2019).[20]

The Senate Intelligence Committee also spent three years investigating Russia's impact on the election. The Committee has released four volumes (of a five volume) report from this investigation. *See* Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election.[21] In the third volume of the Committee's report, the Committee recommended that in the future, the "public should be informed as soon as possible . . . even if the information is incomplete" of any detected foreign threats to elections. Senate Select Committee on Intelligence, *Russian Active Measures*

[20] https://news.yahoo.com/dhs-warns-russia-influence-2020-elections-170005501.html.
[21] https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures.

Campaigns and Interference in the 2016 U.S. Election, Volume 3: U.S. Government Response to Russian Activities 45 (2020).[22]

There is a profound and urgent public interest in the release of records in possession of the DHS sought by EPIC concerning the vulnerabilities of and threats to our election systems. The release of these records is necessary for the public to evaluate DHS's response to past incidents, to assess future threats to election systems, and to ensure the accountability of the federal agency with the legal authority to safeguard our election systems. With the 2020 Presidential Election mere months away, it is crucial that the public understands the DHS's assessments of the vulnerability of election systems. The public should be able to know what steps the agency has taken to protect these systems and to protect our democratic institutions.

III. EPIC's FOIA Request and Scope of Issues in Dispute

In response to the Government's assessment that Russia had conducted a sophisticated cyber interference campaign against the 2016 Election and the designation of election systems as critical infrastructure, EPIC submitted a FOIA request ("EPIC's FOIA Request") to the DHS on March 31, 2017. The FOIA request was transferred to the NPPD, now CISA, for direct response.

Specifically, EPIC sought:

> (A) Any document, record, memo, correspondence, or other communication or any portion of any such communication of the Department of Homeland Security that refers 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 or at the direction of 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.
>
> (2) Dissemination by the Department of information regarding interference with the elections for Federal office held in 2016 by or

[22] https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume3.pdf.

at the direction of 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 United States persons and institutions by or 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 used by Russian intelligence services to compromise and exploit networks and infrastructure associated with the elections for Federal office held in 2016 issued by the Secretary of Homeland Security and the 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 Representatives pursuant to House Resolution 235.

After constructively exhausting its administrative remedies, EPIC filed suit on October 4, 2017. *See* Compl. The parties conferred and agreed to a processing schedule. Proposed Briefing Schedule, ECF No. 8. After CISA, taking over the role of NPPD for direct response to EPIC's FOIA Request, completed the processing of records, the parties conferred to narrow the scope of issues in dispute. *See* Joint Status Report, ECF No. 21. In an attempt to narrow the issues in dispute, CISA conducted a supplemental search and agreed to revisit some of the fully withheld pages to determine if additional portions of the record could be released. *Id.* at ¶ 5. EPIC also agreed to narrow the scope of its request to records that were not drafts or e-mail chains in an effort to exclude materials that may be subject to Exemption 5. *See* Joint Status Report ¶ 5, ECF No. 14. CISA provided a draft *Vaughn* Index with information about records withheld in full that are not drafts or e-mail chains. Joint Status Report ¶ 5, ECF No. 21.

After reviewing the production and the draft *Vaughn* Index, EPIC requested that CISA reprocess 16 documents (94 pages) because it believed that additional information could be released. Joint Status Report ¶ 7, ECF No. 22. These 16 documents fall into four categories: (1) documents concerning contacts between the DHS and State Election Officials; (2) Election Task

Force meeting minutes; (3) documents about risk characterizations and analysis on interference in election infrastructure; and (4) incident reports about the vulnerabilities in election systems. *Id*. ¶ 5. CISA agreed to reprocess these 16 documents. *Id*. at ¶ 7. EPIC explained that there is a strong public interest in making these records available to the public because the documents relate to the interference and vulnerabilities of our election systems. Joint Status Report ¶ 7, ECF No. 21. EPIC told the agency that "the release of this information is critical for the public to understand past cyber incidents and vulnerabilities to election systems and whether or not the DHS has worked with states to ensure these systems are secure going forward." *Id.*

On February 14, 2020, the DHS informed EPIC that it had reprocessed the 16 documents and was releasing three pages in full, withholding five pages in part, and withholding 80 pages in full under Exemption 5, 6, and/or 7(E). Joint Status Report ¶ 5, ECF No. 23. DHS also informed EPIC that two of the documents withheld in full were duplicates. *Id*. at ¶ 2 n.2. One document required further consultation with another agency and was eventually released in full. *Id*. at ¶ 6. After reviewing the agency's response, EPIC informed the agency that it would narrow the scope of issues in dispute to the 12 documents and planned to challenge the DHS's Exemption 5 and 7(E) withholdings, as well as the agency's failure to release all reasonably segregable portions of the records. *Id*. at ¶ 7. EPIC is not challenging the adequacy of the agency's search or any other withholdings. *Id*.

ARGUMENT

The FOIA was enacted "to facilitate public access to Government documents" and "was designed to pierce the veil of administrative secrecy and to open agency action to the light of public scrutiny." *Citizens for Responsibility and Ethics in Washington v. DOJ*, 746 F.3d 1082,1088 (D.C. Cir. 2014) [hereinafter CREW] (quoting *Dep't of State v. Ray*, 502 U.S. 164,

173 (1991)). The underlying purpose of the FOIA is "to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed." *EPIC v. DHS*, 999 F. Supp. 2d 24, 29 (D.D.C. 2013) (quoting *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 152 (1989)). The FOIA "reflects a general philosophy of full agency disclosure unless information is exempted under clearly delineated statutory language." *Judicial Watch, Inc. v. DHS*, 895 F.3d 770, 775 (D.C. Cir. 2018) (internal quotation marks omitted). "Designed to facilitate public access to Government documents, FOIA requires federal agencies to disclose information to the public upon reasonable request unless the records at issue fall within specifically delineated exemptions." *Reporters Comm. for Freedom of Press v. FBI*, 877 F.3d 399, 401 (D.C. Cir. 2017) (internal quotations omitted). "In enacting FOIA, Congress struck the balance it thought right—generally favoring disclosure, subject only to a handful of specified exemptions—and did so across the length and breadth of the Federal Government." *Milner v. Dep't of the Navy*, 562 U.S. 562, 572 (2011). As a result, the FOIA "mandates a strong presumption in favor of disclosure." *EPIC v. DOJ*, 511 F. Supp. 2d 56, 64 (D.D.C. 2007) (internal citations omitted).

The FOIA specifies that certain categories of information may be exempt from disclosure, "[b]ut these limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act." *ACLU v. DOJ*, 655 F.3d 1, 5 (D.C. Cir. 2011) (quoting *Nat'l Ass'n of Home Builders v. Norton*, 309 F.3d 26, 32 (D.C. Cir. 2002)). Therefore, the FOIA exemptions "must be narrowly construed." *Id*. The statute's "goal is broad disclosure," and the exemptions must be "given a narrow compass." *Milner*, 562 U.S. at 571. Furthermore, "the burden is on the agency to sustain its action." 5 U.S.C. § 552(a)(4)(B); *see also EPIC v. DHS*, 384 F. Supp. 2d 100, 106 (D.D.C. 2005). Where the government has not carried this

burden, summary judgment in favor of the Plaintiff is appropriate. *DOJ v. Tax Analysts*, 492 U.S. 136, 142 (1989); *see also Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 861 (D.C. Cir. 1980).

I. STANDARD OF REVIEW

Summary judgment may be granted if "the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). "A genuine issue of material fact is one that would change the outcome of the litigation." *EPIC v. DHS*, 999 F. Supp. 2d 24, 28 (D.D.C. 2013) (citing *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986)). FOIA cases are typically decided on motions for summary judgment. *Niskanen Ctr. v. Fed. Energy Regulatory Comm'n*, No. CV 19-125 (JEB), 2020 WL 224515, at *2 (D.D.C. Jan. 15, 2020); *see Brayton v. Office of U.S. Trade Rep.*, 641 F.3d. 521, 527 (D.C. Circ. 2011). A district court reviewing a motion for summary judgment in a FOIA case conducts a *de novo* review of the record. 5 U.S.C. § 552(a)(4)(B); *DOJ v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 755 (1989). When reviewing an agency's motion for summary judgment, the court must "analyze all underlying facts and inferences in the light most favorable to the FOIA requester," and therefore "summary judgment for an agency is only appropriate after the agency proves that it has 'fully discharged its [FOIA] obligations.'" *Neuman v. United States*, 70 F. Supp. 3d 416, 421 (D.D.C. 2014) (citing *Moore v. Aspin*, 916 F. Supp. 32, 35 (D.D.C. 1996)).

The burden falls on the agency to prove that it has complied with its obligations under FOIA. 5 U.S.C. § 552(a)(4)(B). *See also Valencia-Lucena v. U.S. Coast Guard*, 180 F.3d 321, 326 (D.C. Cir. 1999) (quoting *Oglesby v. U.S. Dep't of Army*, 920 F.2d 57, 68 (D.C. Cir. 1990)). Where the government has not carried this burden, summary judgment in favor of the Plaintiff is appropriate. *See, e.g.*, *Tax Analysts*, 492 U.S. at 142; *Coastal States*, 617 F.2d at 861.

II. EPIC IS ENTITLED TO PARTIAL SUMMARY JUDGMENT

EPIC is entitled to partial summary judgment as to the 12 documents identified in the *Vaughn* index because the agency has unlawfully withheld material that does not fall within any FOIA exemptions.

The FOIA provides that every government agency shall, "upon any request which (i) reasonably describes such records and (ii) is made in accordance with published rules[,] . . . make the records promptly available to any person." 5 U.S.C. § 552(a)(3)(A). In a FOIA case, the "agency bears the burden of establishing that an exemption applies." *PETA v. NIH*, 745 F.3d 535, 540 (D.C. Cir. 2014). In some cases, the agency may carry its burden by submitting affidavits that "describe the documents and 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 evidence of agency bad faith." *Ullah v. CIA*, No. CV 18-2785 (JEB), 2020 WL 248937, at *2 (D.D.C. Jan. 16, 2020) (quoting *Military Audit Project v. Casey*, 656 F.2d 724, 738 (D.C. Cir. 1981)) (internal quotations omitted). However, it is not sufficient for an agency to provide "vague, conclusory affidavits, or those that merely paraphrase the words of a statute." *Church of Scientology of Cal., Inc. v. Turner*, 662 F.2d 784, 787 (D.C. Cir. 1980) (per curiam). The agency must "provid[e] a sufficiently detailed description of the exemption, the portion(s) of documents to which it applies, and justification as to why the exemption is relevant . . . ." *Shapiro v. DOJ*, 293 F. Supp. 3d 99, 109 (D.D.C. 2018), *rev'd in part, vacated in part on alternative grounds,* 944 F.3d 940 (D.C. Cir. 2019). The agency affidavits must provide "'the kind of detailed, scrupulous description [of the withheld documents] that enables a District Court judge to perform a de novo review.'" *Brown v. FBI*, 873 F. Supp. 2d 388, 401 (D.D.C. 2012).

Further, the FOIA's segregability requirement ensures that agencies release all portions of responsive documents that would not cause harm under one of the Exemptions, thus assuring that agencies comply with the statute in a precise and granular fashion. The D.C. Circuit has emphasized that the focus of the FOIA "is information, not documents." *Stolt-Nielson Transp. Group Ltd. v. United States*, 534 F.3d 728, 733–34 (D.C. Cir. 2008) (citing *Mead Data Ctr., Inc. v. U.S. Dep't of Air Force*, 566 F.2d 242, 260 (1977)). As a result, the FOIA imposes an affirmative obligation to segregate and release all non-exempt materials; "an agency cannot justify withholding an entire document simply by showing that it contains some exempt material." *Id.*; *see also* 5 U.S.C. § 552(b).

The agency's obligation to release segregable, non-exempt portions of responsive records is well established, and the burden is on the agency to prove that they have satisfied this requirement. The FOIA states:

> Any 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. The amount of information deleted, and the exemption under which the deletion is made, shall be indicated on the released portion of the record, unless including that indication would harm an interest protected by the exemption in this subsection under which the deletion is made.

5 U.S.C. § 552(b). If the agency fails to "provide 'specific and detailed proof that disclosure would defeat, rather than further, the purposes of the FOIA,'" the agency has not met its statutory obligation. *Morley v. CIA*, 508 F.3d 1108, 1127 (D.C. Cir. 2007). If the context and description of a document makes clear that the document contains reasonably segregable portions of information, the agency cannot simply recite the statutory standard and meet its burden.

But even a detailed description may not be enough in all cases. Courts can require *in camera* inspection of records in order to determine whether any segregable factual material

exists if "an agency's affidavits merely state in conclusory terms that documents are exempt from disclosure." *Quinon v. FBI*, 86 F.3d 1222, 1229 (D.C. Cir. 1996); *see also Meeropol v. Meese,* 790 F.2d 942, 958 (D.C. Cir. 1986) ("[A] finding of bad faith or contrary evidence is not a prerequisite to in camera review; a trial judge may order such an inspection 'on the basis of an uneasiness, on a doubt he wants satisfied before he takes responsibility for a de novo determination.'") (citing *Ray v. Turner,* 587 F.2d 1187, 1195 (D.C. Cir. 1978)). EPIC will discuss segregability in each exemption section.

A. The DHS Has Not Met Its Burden to Withhold Material Pursuant to Exemption 5

The FOIA Exemption 5 permits the withholding 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). To qualify for Exemption 5, responsive records must come from a government agency and must fall within a litigation privilege against discovery. *Dep't of Interior v. Klamath Water Users Protective Ass'n*, 532 U.S. 1, 8 (2001). Privileges incorporated by Exemption 5 include the deliberative process privilege, which "protects agency documents that are both predecisional and deliberative," *Judicial Watch, Inc. v. FDA*, 449 F.3d 141, 151 (D.C. Cir. 2006), and the attorney-client and work-product privileges.

The DHS has invoked the deliberative process privilege for each of the 12 documents at issue, but that privilege does not apply to the portions of these documents that contain factual information, formal assessments completed by the agency, and other non-deliberative materials. The privilege is intended "to enhance the quality of agency decisions by protecting open and frank discussion among those who make them within the Government." *Am. Immigration Council v. DHS*, 21 F. Supp. 3d 60, 75 (D.D.C. 2014) (internal quotations omitted). In order to properly withhold material under Exemption 5, the agency must provide evidence of "what

deliberative process [was] involved, and the role played by the documents in issue in the course of that process." *Senate of P.R. v. DOJ,* 823 F.2d 574, 585–86 (D.C. Cir. 1987). "Merely stamping on the face of the documents that they are subject to the deliberative process privilege is not sufficient." *Judicial Watch, Inc. v. DOJ*, 20 F. Supp. 3d 260, 269 (D.D.C. 2014). A record is "deliberative" if it reflects the give-and-take of the consultative process. *Coastal States*, 617 F.2d at 866.

Factual materials are not generally not protected under Exemption 5. *Leopold v. CIA*, 89 F. Supp. 3d 12, 22 (D.D.C. 2015) ("Straightforward, mechanical recitations of fact . . . will generally fall outside of the privilege."); *Pub. Citizen, Inc. v. OMB*, 598 F.3d 865, 876 (D.C. Cir. 2010) ("[A]gencies must disclose those portions of predecisional and deliberative documents that contain factual information that does not 'inevitably reveal the government's deliberations.'").

Under the 2016 FOIA amendments, an agency seeking to withhold material under Exemption 5 must establish that it "reasonably foresees that disclosure would harm an interest protect by an exemption . . . or disclosure is prohibited by law." 5 U.S.C. § 552(a)(8)(A)(i). To satisfy the foreseeable harm requirement, the agency must "articulate both the nature of the harm and the link between the specified harm and specific information contained in the material withheld." *Judicial Watch, Inc. v. U.S. Dep't of Commerce*, 375 F. Supp. 3d 93, 100 (D.D.C. 2019) (internal quotations omitted). An agency cannot meet its FOIA burden by providing conclusory allegations of possible harm, rather "[i]t must show by specific and detailed proof that disclosure would defeat, rather than further, the purposes of the FOIA." *Mead Data Ctr.*, 566 F.2d at 258.

The twelve records at issue fall into four categories: (i) summaries of meetings between DHS and State Election Officials; (ii) Election Task Force meeting minutes; (iii) a report titled

"Election Infrastructure Cyber Risk Characterization Report; and (iv) incident reports. Declaration of James Holzer ("Holzer Decl.") ¶¶ 19–22. The DHS claims that all twelve of these records are subject to the deliberative process privilege. But the agency has not provided evidence of specific decisions to which these records were pre-decisional and has not shown that these records were part of the give-and-take of the deliberative process. The agency has a responsibility to protect election infrastructure in coordination with state election officials, but that duty does not justify withholding materials from the public concerning the scope of election vulnerabilities and the severity of past incidents. Indeed, the only way that we can learn from past mistakes is to study them, and there is no way for cybersecurity experts and members of the public to oversee DHS's work carrying out its election cybersecurity mandate unless they have access to the agency's facts and assessments.

The records at issue include the agency's assessments and evaluations of cybersecurity incidents and vulnerabilities in election systems in 2016 and 2017. This information is of critical public importance and withholding it does not serve the purposes of the deliberative process privilege. The records also clearly contain factual information that cannot be withheld under Exemption 5 even if the documents themselves were used in a deliberative process. The Holzer declaration does not articulate any specific harm that would occur if the agency this information. The twelve records that the DHS is withholding are not subject to the deliberative process privilege, and the records must therefore be disclosed.

i. Contacts between the DHS and State Election Officials

The DHS has not established that the category of records about contacts between DHS and state election officials is subject to Exemption 5's deliberative process privilege. All of the documents in this category contain segregable, factual information that is not deliberative. The

three documents in this category are either spreadsheets or charts that describe or summarize contacts between the DHS and state election officials. One document, titled "Weekly Summary for Meetings with Elections Infrastructure Officials," consists of excel spreadsheets that summarize of meetings between the agency and state officials. EPIC v. DHS Vaughn Index, ECF No. 26-2 page 13, at 1–2 (describing documents NPPD 000351-NPPD 000360, NPPD 000401-NPPD 000410). Another document consists of two spreadsheets "describing engagement" with states, including the agency's "understanding of the status of vulnerabilities in the states' election infrastructure." EPIC v. DHS Vaughn Index 1 (describing documents NPPD 000419, NPPD 000944). The last document in this category, titled "State Outreach Status – DHS Election Infrastructure Campaign," is an "interim report chart" that was used as an "internal tracking document" that recorded the status of the agency's outreach to states regarding risk vulnerability and "cyber hygiene" assessments. EPIC v. DHS Vaughn Index 2 (describing document NPPD 000967). While the agency claims that the documents contain "staff assessments of the meetings" and "recommendations for future action," the charts and spreadsheets are not deliberative material that can be withheld in full under Exemption 5. Holzer Decl. ¶ 19. The DHS could segregate and withhold any opinions and recommendations of agency officials related to specific deliberations while still releasing factual summaries of meetings with election officials.

These summaries of meetings with election officials are not deliberative merely because they describe "discussion points" and "areas of concern." EPIC v. DHS Vaughn Index 1 (describing documents NPPD 000419, NPPD 000944). Any discussions with state election officials were not inter-agency communications and thus descriptions of those communications are not subject to privilege. Similarly, a chart of the status of NPPD's outreach to states

regarding risk vulnerability and cyber hygiene assessments of state election infrastructure is not deliberative as it merely contains factual material regarding the progress of the agency's outreach strategy. EPIC v. DHS Vaughn Index 2 (describing document NPPD 000967). The DHS characterizes this chart as a "progress report chart," *Id.*, which is not a deliberative document because it does not reflect the "give and take" of the agency consultation process. *Coastal States*, 617 F.2d at 866. The other document, a spreadsheet describing engagement with 22 states and a spreadsheet describing engagement with three states included assessments of "then-current engagement" with states and the NPPD's "understanding of the status of vulnerabilities in the states' election infrastructure," contain segregable factual material. EPIC v. DHS Vaughn Index, ECF No. 26-2, at 13 (describing documents NPPD 000419, NPPD 000944). This information in the spreadsheet merely describes the agency's engagement with states, which would not itself reveal the internal deliberations of agency staff.

In *Judicial Watch, Inc. v. U.S. Dep't of State*, the court found that summaries of phone calls between the President of the United States and the President of Libya and Egypt in the aftermath of the Benghazi attack were not pre-decisional because they were meant to inform State Department Officials facts that could have been relevant to perform their duties but did not suggest an actual use in a decision-making process about how to respond to a national security crisis. 241 F. Supp. 3d 174, 185 (D.D.C.), *amended on reconsideration*, 282 F. Supp. 3d 338 (D.D.C. 2017). And the court in *Judicial Watch* made clear that a document does not contain deliberative material merely because staff selected facts to be included in a summary. *Id*. Like the summaries of calls in *Judicial Watch*, the meeting summaries, engagement spreadsheet, and interim progress report chart are reporting for informational purposes and there was no back and

forth, no give and take, or request for comment or input from DHS officials on a particular matter.

The DHS has also not explained why releasing this material would cause a foreseeable harm. The agency's claim that the release of this information "would give the public an erroneous understanding of the basis for agency decisions" does not meet the foreseeable harm standard. The public's understanding of the basis for an agency decision is not an interest that is protected by Exemption 5. There is no evidence that the release of this information would harm the ability of the agency staff to communicate in a frank and open manner to agency leadership.

Moreover, the agency fails to adequately support its assertion that releasing the material would harm the deliberative process. In *Judicial Watch v. Department of Commerce*, the court found that the Commerce Department failed to justify its withholdings under the deliberative process privilege because the agency's speculative declarations failed to show how to the release of communications between a National Oceanic and Atmospheric Administration ("NOAA") scientist and the director of NOAA's Office of Science and Technology Policy could chill speech. 375 F. Supp. 3d 93, 100 (D.D.C. 2019). The Commerce Department affidavit's provided boiler plate, general explanations of the possibility of the "chilling effect" of agency speech but the explanations fell short of articulating the link between the harm and the specific information contained in the material withheld. *Judicial Watch*, 375 F. Supp. 3d at 100. The court stated that the FOIA "requires more than speculation." *Id.* at 101. The DHS's declarations in this case suffer from the same fatal flaw; the agency has provided nothing more than a recitation of the legal standard, stating that release would "inhibit agency staff's ability to communicate frank, current, non-final assessments to agency leadership." Holzer Decl. ¶ 19.

There is a strong public interest that favors disclosure in this case and the agency is not prohibited from releasing these records. Accordingly, the court should not permit the withholding because DHS cannot provide evidence of specific harm that would result from disclosure. CISA is tasked with protecting election infrastructure yet it has not proactively released any new information about the current status of engagement with state election officials. When the DHS acknowledged that 21 states had been targeted by Russia, a year after detecting the incident, many state officials were surprised to learn that they had been targeted by foreign hackers. Some states expressed disappointment and distrust towards the federal government for not communicating known cyber incidents earlier. *See* Geoff Mulvihill & Jake Pearson, *Federal Government Notifies 21 States of Election Hacking*, Assoc. Press (Sept. 22, 2017).[23] Other documents released to EPIC in this case revealed that the agency recognized the need to repair trust with states and encourage greater utilization of CISA's resources to protect state elections. Additionally, a 2019 Inspectors General report found that the "state and local officials' historic mistrust of Federal government assistance restrict[ed] DHS's efforts to provide the services and assessments needed to secure the election infrastructure." DHS OIG Report, *supra*, at 12. Release of information about meetings between the agency and state officials will allow the public to gain a deeper understanding of the relationship between CISA and states and the extent of CISA's support to safeguard state election systems.

ii. Election Task Force meeting minutes

The DHS has not established that Election Task Force meeting minutes are deliberative. The agency's description of the Election Task Force meeting minutes makes clear that these

[23] https://apnews.com/cb8a753a9b0948589cc372a3c037a567/Federal-government-notifies-21-states-of-election-hacking.

records include reports and status updates from task force members; the minutes also presumably include other functional details such as rosters of individuals who attended the meeting and other agenda items. Holzer Decl. ¶ 20. The status of a specific action, task, or project that involved the Election Security Task Force is not deliberative because it does not reflect the "give and take" of a deliberative process. Solely conveying the progress of a task does not involve an exercise the type of judgement by agency employees that should be privileged.

Meeting minutes undoubtedly include information that is not deliberative and can be segregated. The agency has not shown that the meetings concerned specific agency decisions or explained how the meeting minutes would reveal the give and take of a deliberative process. But even where meeting minutes do concern a deliberative process, courts have ordered release of segregable portionsof those minutes. In *Judicial Watch, Inc. v. Department of Treasury*, the court held that disclosure of the headers at the top of the Treasury's Office of Financial Stability ("OFS") committee meeting minutes, along with the names of the committee members present, and the names of observers were reasonably segregable from the actual meeting minutes. 796 F. Supp. 2d 13, 29–30 (D.D.C. 2011). And that was after the court reviewed the minutes and concluded that they *did* contain deliberative material. Specifically, the OFS committee meeting minutes summarized deliberations of the committee regarding pending Capital Purchase Program applications. *Id.* at 28.

Unlike the deliberations about pending Capital Purchase Programs applications in *Judicial Watch*, the DHS has not established that the Election Security Task Force was engaged in any decisionmaking process or that their minutes would reveal deliberations. The agency only vaguely states that the meetings were "in furtherance of the Task Force's goal of assessing risk to election infrastructure." Holzer Decl. ¶ 20. Because these Election Task Force meetings do not

concern agency deliberation over a specific decision making process, these minutes should not be privileged. Even if the minutes are privileged, the DHS has an obligation to release reasonably segregable material. *See Judicial Watch*, 796 F. Supp. 2d 13 at 29; *Ctr. for Pub. Integrity v. United States Dep't of Commerce*, 401 F. Supp. 3d 108, 120 (D.D.C. 2019) (finding that letter and e-mail header information, including names of senders and recipients, titles, and subject matter descriptions, could be reasonably segregated and is non-exempt).

Moreover, the agency has not identified any harm that disclosure would cause to a specific deliberative process. The DHS generalizes that the release of this information would have a "chilling effect on the deliberative discussions of meeting of *agency task forces*." Holzer Decl. ¶ 20 (emphasis added). The Election Task Force was a temporary mechanism and was disbanded. Holzer Decl. ¶ 20. The release of the Task Force meeting minutes would not chill any actions by task force members because the task force does not exist. The DHS's vague description of the contents of the task force minutes, Holzer Decl. ¶ 20, are not sufficient to establish that the records were part of a specific decision making process or that they contain the type of "given and take" communications that constitute deliberative materials.

Other courts have held that similarly vague agency descriptions are insufficient to support an Exemption 5 withholding. In *Electronic Frontier Foundation v. Department of Justice*, the court found that the agency could not withhold records about the United States-European Union High Level Contact Group ("HLCG"). 826 F. Supp. 2d 157, 168 (D.D.C. 2011). In one instance, the agency withheld e-mail messages "wherein senior [DOJ] officials seek and receive advice, and discuss questions, developments, and potential ramifications with respect to the HLCG deliberations" and in the supporting declaration adds that the e-mails "consist of back and forth discussions, forwards, and spinoff discussions, in which [DOJ officials] exchange any thoughts,

ideas, or guidance they deem appropriate regarding the U.S.[']s . . . negotiation position on HLCG matters. These officials analyze and prepare for EU negotiating positions, and work amongst themselves to promote [DOJ] and U.S. foreign interests in these foreign negotiations." *Id.* at 168 (internal quotations omitted). The court found that the description was inadequate because "vague references to 'HLCG matters' and 'deliberations' provides little context to the court and the plaintiff, given that the HLCG negotiations occurred on various instances throughout 2008 and 2009." *Id*. Like the vague references from the agency affidavits in *EFF v. DOJ*, the DHS's description of the context of the Election Task Force meeting minutes does not provide context to what deliberative process was involved.

iii. Election Infrastructure Cyber Risk Characterization Report

The DHS's assessment of cyber risks, which was completed in September 2016, is a final assessment and not a pre-decisional document. The parties already agreed that the remaining documents at issue in this case are final records, which do not include drafts that include tracked changes or any other deliberative material. *See* Joint Status Report ¶ 7, ECF No. 21. The Election Infrastructure Cyber Risk Characterization Report is therefore a final report prepared by NPPD. A final report is not pre-decisional. The report, dated September 2016, contained information about the characterization of selection election infrastructure vulnerabilities and the likelihood of cyber intrusions at the time the report was prepared. EPIC v. DHS Vaughn Index 2 (describing document (NPPD 000926-NPPD 000942). While the status of election infrastructure vulnerabilities have changed in the course of four years, the information was final at the time the report was made. As such, the final report is not protected by the deliberative process privileged because it is not pre-decisional.

In *Heartland Alliance for Human Needs & Human Rights v. United States Department of Homeland Sec*., the court held that statistical reports related to the agency's immigration enforcement programs were not protected under the deliberative process privilege because, while the reports were drafts and contained edits, the agency did not articulate a decision making process that would make it pre-decisional. 291 F. Supp. 3d 69, 79 (D.D.C. 2018). The agency in Heartland repeated a vague explanation as to why the draft documents were pre-decisional and the court determined that such an explanation was insufficient to exempt material under Exemption 5. *Id*. at 80. Here, the DHS has similarly provided vague explanations as to why the Election Infrastructure Cyber Risk Characterization is pre-decisional.

Additionally, the agency has not identified any decision making process linked to this report. Merely stating that the report was used to "support DHS's planning to enhance security of election infrastructure" and to "aid decisions" for leadership planning does not specify what type of leadership planning decision or consultation was made at the time. The DHS's affidavit is not specific in what the deliberative process was, other than for "leadership planning," and does not establish a give and take between agency staff and leadership. Holzer Decl. ¶ 21. The agency has therefore not satisfied the Exemption 5 burden to withhold the Election Infrastructure Risk Characterization Report because it is a final report that is not deliberative or pre-decisional.

iv. Incident Reports

As mentioned above, the parties agreed that the remaining issues in dispute involve records that are not drafts or e-mails. *See* Joint Status Report ¶ 7, ECF No. 21. While the DHS states that these are "non-final" assessments, the incident reports are final reports and the agency has not argued that these reports are drafts or subject to revision. Holzer Decl. ¶ 22.

The DHS has not provided sufficient evidence to show that these incident reports are pre-decisional. The DHS merely generalizes the agency decision making process. Providing records for "situational awareness and oversight" encompasses the general regulatory functions of an agency, rather than a specific agency decision. Holzer Decl. ¶ 22. For example, a preliminary digital media analysis report titled "National Cybersecurity and Communications Integration Center (NCCIC)/United States Computer Readiness Teams (US-CERT) Preliminary Digital Media Analysis Report regarding cyber incident" was prepared for another federal agency that included findings and recommended actions. EPIC v. DHS Vaughn Index 3 (describing documents NPPD 001115-NPPD 001119). The DHS states vaguely that the report was prepared "for the agency's deliberation and potential implementation" but does not specify what potential agency decision this report predates. *Id.* This vague reasoning does not hold water under Exemption 5 to satisfy the agency's burden to tie the records to a specific deliberative process.

The DHS also has not provided sufficient evidence to show that these incident reports are deliberative. For example, a chart titled "Election Related State Incidents" lists information "as the agency received it." EPIC v. DHS Vaughn Index 3 (describing documents NPPD 000963-NPPD 000966). The information in the chart is factual, received from an outside party, and would not constitute the opinions or recommendations of agency employees. Similarly, another document is comprised of a timeline of e-mails and incident reports that was created as "a tool for oversight and awareness of staff's work." EPIC v. DHS Vaughn Index 4 (describing document NPPD 001095-NPPD 001106). The timeline of e-mails and incident reports do not reflect open and frank discussions between staff and leadership, or provide recommendations or deliberations.

Moreover, any non-deliberative information within these incident reports can be segregated and released because factual information, for instance, are not protected under Exemption 5. For example, one of the untitled reports include an incident summary and state vulnerability scanning and assessments. EPIC v. DHS Vaughn Index 3 (describing document NPPD 000962). The incident summary and state vulnerability assessments do not contain agency deliberations. Similarly, a list of election related incidents in chart form is not deliberative as it charts information "as the agency received it." EPIC v. DHS Vaughn Index, ECF No. 26-2, at 15 (describing document NPPD 000963-NPPD 000966). The chart was used for briefing on election-related incidents and do not contain the thoughts or opinions of agency employees in the course of deliberating an agency action. Likewise, the agency withheld a timeline of emails and incident reports received by CISA. EPIC v. DHS Vaughn Index, ECF No. 26-2, at 16 (describing document NPPD 001095-NPPD 001106). The information in the timeline was information received by the agency and includes select facts, summaries between the agency and states, and assessments of communications with outside parties. *Id.* This is factual information not protected by the deliberative process privilege because it does not reflect the thoughts, opinions, and pre-decisional impressions of employees.

The agency has not articulated the nature of the harm and linked the specific harm to the information in the withheld records. The DHS notes that the information contained in these reports would "mislead the public." Holzer Decl. ¶ 22. Misleading the public is not a foreseeable harm protected under Exemption 5. Nothing prevents the DHS from warning the public that the record contains non-verified information. Information compiled for a specific time period still serves the public interest in understanding the agency's decision making process. The DHS also speculates that disclosure would "foreseeably harm CISA's ability to community clearly and

frankly with other federal partners and would harm CISA staff's ability to provide transparent communication and assessments to CISA leadership." Holzer Decl. ¶ 22. If the Court finds that there are deliberative materials within the documents, the Court should at least order the agency to release reasonably segregable portions of these incident reports because there is factual information that is not protected under Exemption 5.

v. The DHS has failed to release reasonable segregable portions of responsive records

The discovery privileges incorporated by Exemption 5 do not override the segregability obligation, but instead "work in conjunction" to ensure that agencies satisfy their duty to produce non-exempt materials even when they appear in the same record as protected materials. *Judicial Watch, Inc. v. DOJ*, 432 F.3d 366, 369 (D.C. Cir. 2005). "[A] blanket declaration that all facts are so intertwined," conversely, is not sufficient to meet this burden." *Nat'l Whistleblower Ctr. v. HHS*, 903 F. Supp. 2d 59, 70 (D.D.C. 2012) (internal quotations omitted).

The DHS's affidavit and *Vaughn* index support the conclusion that the agency has not released all non-exempt, reasonably segregable material. For instance, the contents of the Task Force meeting minutes include "reports" and "status updates." Holzer Decl. ¶ 20. These meeting minutes, [like those in Judicial Watch and CPI], contain factual and descriptive information that is not part of any deliberative process. The incident reports and Election Infrastructure and Cyber Risk Characterization Report are final reports that are not exempt under the deliberative process privilege because the documents are no longer pre-decisional. By withholding all the documents in full, the agency is improperly withholding reasonably segregable information.

Lastly, the agency holds this privilege but it has the discretion to waive the privilege if it chooses to do so. The documents at issue are in the public's interest because CISA has not released new information about how it has engaged with states and assessed their election

infrastructure. The public interest in understanding past cyber incidents and known vulnerabilities in the election systems and understanding how CISA is worked with states to address these vulnerabilities greatly outweighs the harm to the deliberative process privilege. CISA's mission is to help states, on a voluntary basis, with securing their election systems. It is critical that the public understands the extent of these endeavors given that foreign threats are expected to target the upcoming 2020 Presidential Election.

B. The DHS has not met its burden to withhold material pursuant to Exemption 7(E)

Exemption 7(E) protects from disclosure records 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). To withhold records under Exemption 7(E) an agency must satisfy two statutory requirements. First, the agency must show that the record was "compiled for law enforcement purposes." § 552(b)(7); *see John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 153 (1989) ("Before it may invoke [Exemption 7], the Government has the burden of proving the existence of such a compilation for such a purpose."); *Pub. Empls. for Envtl. Responsibility v. U.S. Section, Int'l Boundary and Water Comm'n*, 740 F.3d 195, 202–03 (D.C. Cir. 2014) [hereinafter *PEER*]. Second, the agency must show that production would either "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); *see PEER*, 740 F.3d at 204. And while the statute does not impose a "highly specific burden of showing how the law will be circumvented," the agency cannot rely on

"vaguely worded categorical description[s]." *New Orleans Workers' Ctr. for Racial Justice v. ICE*, 373 F. Supp. 3d 16, 64–65 (D.D.C. 2019).

As the *New Orleans* court recently explained:

> Although the standard for making this showing "is a fairly low hurdle in this Circuit, [ ] it is not a toothless [one]," and "the [g]overnment cannot simply cite Exemption 7(E) and expect the court to rubber stamp its withholdings." *Long II*, 279 F. Supp. 3d at 234; *Campbell*, 164 F.3d at 32 (a court's review of an agency's withholding under Exemption 7(E) is not "vacuous"). Rather, "[c]ourts have a responsibility to ensure that an agency is not simply manufacturing an artificial risk and that the agency's proffered risk assessment is rooted in facts." *Long v. ICE*, 149 F. Supp. 3d 39, 53 (D.D.C. 2015) (Long I). "At a minimum, the [g]overnment must show that its stated expectation of risk is reasonable." *Long II*, 279 F. Supp. 3d at 234. And, "[a]n affidavit that contains merely a categorical description of redacted material coupled with categorical indication of anticipated consequences of disclosure is clearly inadequate." *Campbell*, 164 F.3d at 30 (internal citation and quotation marks omitted).

Id. at 66.

To satisfy the second prong, the agency must provide a "relatively detailed justification" for each record that permits the reviewing court to make a meaningful assessment of the redactions. *Strunk v. U.S. Dep't of State*, 845 F. Supp. 2d 38, 47 (D.D.C. 2012). This detailed justification includes:

> 1) a description of the technique or procedure at issue in each document, 2) a reasonably detailed explanation of the context in which the technique is used, 3) an exploration of why the technique or procedure is not generally known to the public, and 4) an assessment of the way(s) in which individuals could possibly circumvent the law if the information were disclosed.

Am. Immigration Council v. DHS, 950 F. Supp. 2d 221, 247 (D.D.C. 2013). Clearing the "low hurdle" of demonstrating a risk of circumvention of the law is not sufficient for an agency to meet its burden under Exemption 7(E); the agency must first show that production of the records at issue would *disclose techniques and procedures* for law enforcement investigations. *EPIC v. CBP*, 160 F. Supp. 3d 354, 359 (D.D.C. 2016). Moreover, a "near-verbatim recitation of the statutory standard is inadequate." *CREW*, 746 F.3d at 1102 (D.C. Cir. 2014).

The DHS withheld eight records under Exemption 7(E): a spreadsheet describing engagement with State Election Officials EPIC v. DHS Vaughn Index, ECF No. 26-2, at 13 (describing documents NPPD 000419, NPPD 000944); a chart of the status of CISA's outreach to states regarding risk vulnerability and cyber hygiene assessments for election infrastructure *Id.* at 14 (describing document NPPD 000967); the Election Infrastructure Cyber Risk Characterization report *Id.* (describing document NPPD 00926-NPPD 000942); an untitled report sent by the National Cybersecurity and Communications Integration Center ("NCCIC") regarding actions to be taken ahead of Election Day *Id.* at 15 (describing document NPPD 000962); a list of election related incidents *Id.* (describing document NPPD 000963-NPPD 000966); a preliminary digital media analysis report prepared for another agency *Id.* (describing document NPPD 001115-NPPD 001119); and a timeline of emails and incident reports pertaining to election security *Id.* at 16 (describing document NPPD 001095-NPPD 001106). These records would not reveal any law enforcement technique or procedure that is protected by Exemption 7(E). And even if some of these records did contain information met the requirements of 7(E), the agency has an obligation to release reasonably segregable portions of the responsive records—which it has failed to do here. Thus, the agency's withholdings under 7(E) are unlawful.

i. The DHS has not shown that documents reveal a technique, procedure, or guideline that is used for investigations or prosecutions.

In order to satisfy its burden under Exemption 7(E), the DHS "must provide sufficient facts and context to allow the reviewing court to deduce something of the nature of the techniques in question." *Am. Immigration Council v. DHS*, 30 F. Supp. 3d 67, 76 (D.D.C. 2014) (internal quotations omitted). Notably, although the Exemption 7 threshold only requires that the records be compiled for a "law enforcement purpose[]," Exemption 7(E) specifically requires

that the techniques or procedures be for *investigations or prosecutions*. *See PEER*, 740 F.3d at 203; *EPIC v. DHS*, 999 F. Supp. 2d 24, 30 (D.D.C. 2013), *rev'd on other grounds*, 777 F.3d 518 (D.C. Cir. 2015) (stating that Congress "specifically and intentionally chose to remove the investigatory requirement from [the threshold requirement of Exemption 7] and leave it in [for 7(E)]"). Investigations or prosecutions under 7(E) include only "acts by law enforcement *after* or *during* the commission of a crime" and they do not even include "crime-prevention techniques." *EPIC*, 999 F. Supp. 2d at 31 (emphasis added).

Here, the DHS has not shown that the records reveal a technique, procedure, or guideline that is used for law enforcement "investigations or prosecutions." CISA does not have a law enforcement mandate and they do not investigate or prosecute crimes. *See* Cybersecurity and Infrastructure Sec. Agency, *About CISA*.[24] The records at issue include "steps CISA takes to assess and mitigate *risks to election systems*." Holzer Decl. ¶ 25 (emphasis added). Steps taken to assess and mitigate cybersecurity incidents are not "techniques [or procedures for law enforcement investigations or prosecutions," and thus fall outside the scope of Exemption 7(E). At best, CISA's assessment procedures are crime *prevention* techniques, but even that is a stretch given that their mandate is not to prevent crimes (e.g. they are responsible for securing infrastructure from risks even if those risks are non-criminal). This court similarly held in 2013 that the DHS's protocol for the shutdown of wireless networks in emergencies did not involve a law enforcement technique or procedure because the protocol articulated protective measures rather than an investigative technique. *EPIC v. DHS*, 999 F. Supp. 2d 31. The Court interpreted "law enforcement investigations or prosecutions" as referring only to acts "after or during

[24] CISA's mission is to "Lead the National effort to understand and manage cyber and physical risk to [the U.S.'s] critical infrastructure."

commission of a crime, not crime-prevention techniques." *Id.*[25] The techniques and procedures used by CISA to assess vulnerabilities in election systems are similarly not used for law enforcement investigations or procedures. They are risk assessment tools and, at most, help to protect against *future* threats. These techniques are thus not subject to Exemption 7(E).

It is also clear from the description of the records that neither category of withheld reports contains techniques and procedures protected by Exemption 7(E). The Election Infrastructure Cyber Risk Characterization Report assesses "State's election infrastructure vulnerabilities, risks of cyber intrusion and mitigation possibilities." Holzer Decl. ¶ 27. The agency does not represented that this report was made during the course of investigating a crime, nor has the agency represented that the report was used in a criminal investigation or prosecution. The agency merely states that the report contains "nonpublic techniques and procedures" used to evaluate cybersecurity risks. The incident reports similarly contain the agency's assessments of vulnerabilities, which could at most reveal techniques the agency uses to "detect and analyze State infrastructure vulnerabilities." Holzer Decl. ¶ 28. One of these incident reports is a chart that shows "reports of tests of State election infrastructure and vulnerability assessments." Holzer Decl. ¶ 28. These tests and assessments that CISA uses to protect election system infrastructure are not investigatory or prosecutorial techniques.

ii. The DHS has failed to release reasonably segregable portions of responsive records

Agencies have an obligation to release reasonably segregable portions of responsive records. 5 U.S.C. § 552(b). The DHS's motion and supporting declaration show that the agency

[25] Although the Court's ruling in *EPIC v. DHS* was reversed on Exemption 7(F) grounds, the D.C. Circuit did not disturb the Court's holding as to Exemption 7(E). *EPIC v. DHS*, 777 F.3d 518, 528 (D.C. Cir. 2015).

has not met its segregability obligations as to the twelve documents at issue. The agency contends that it conducted a "line-by-line review" of the records and that all withheld 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." Holzer Decl. ¶¶ 30, 32. Yet as previously explained, the documents are not records compiled for law enforcement purposes and would not disclose law enforcement techniques or procedures covered by Exemption 7(E). Indeed, some of the records contain reports, status updates, timelines, and lists of incidents that are not even "techniques or procedures" in the first place. For example, list of election-related incidents in chart form EPIC v. DHS Vaughn Index 3 (describing document NPPD 000963-NPPD 000966) is not a technique or procedure; rather, it is an historical record. The Court should, at a minimum, order the DHS to conduct a more rigorous review of the documents withheld and release all reasonable segregable portions of responsive records.

CONCLUSION

The Court should deny the Defendant's Motion for Partial Summary Judgment and grant EPIC's Motion for Partial Summary Judgment.

Respectfully Submitted,

/s/ Alan Butler
ALAN BUTLER, D.C. Bar #1012128
EPIC General Counsel

ENID ZHOU, D.C. Bar #1632392
EPIC Open Government Counsel

Electronic Privacy Information Center
1519 New Hampshire Ave NW
Washington, DC 20036
202-483-1140

Attorneys for Plaintiff EPIC

Dated: June 24, 2019