IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,	)	
Plaintiff,	)	
v.	)	**Civil Action No. 25-1765 (AHA)**
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY	)	
Defendant.	)	

PLAINTIFF'S PRE-MOTION STATEMENT

Plaintiff, Electronic Privacy Information Center (EPIC), files this Pre-Motion Statement in accordance with the Court's Minute Order entered January 12, 2026. EPIC has brought this Freedom of Information Act lawsuit to compel the Defendant—a non-law enforcement agency—to release an unclassified report drafted by a third-party contractor regarding fundamental security vulnerabilities in the country's communications infrastructure.

This report contains a factual assessment by a non-government entity of cybersecurity risks caused by and inflicted upon non-government entities, and the defendant concedes in its Pre-Motion Statement that the report did not inform any decision by the agency. The document addresses vulnerabilities in the telecommunications industry, which concern corporate entities in the United States that are not properly the subject of the FOIA privacy exemption. The agency has not established facts that meet the threshold for any of the legal exemptions to the FOIA that it asserts, and its continued refusal to release the document as required by law, despite the fact that agency officials publicly committed to release it last year, is clear evidence of bad faith.

EPIC filed the underlying FOIA request for the release of this report on March 12, 2024. The agency provided a final response on November 19, 2024, claiming that the entire report was exempt from disclosure under 5 U.S.C. § 552(b)(5) and that no segregable portion could be released. EPIC filed a timely appeal of this determination and then filed suit in June of 2025 after the agency failed to respond. Shortly after EPIC filed suit, the agency publicly committed to release the full report in response to a congressional inquiry. *See, e.g.*, David DiMolfetta, *CISA to release telecom security report as its director nominee nears confirmation*, Nextgov/FCW (July 29, 2025).[1] On information and belief, EPIC asserts that agency staff had even processed a version of the report for public release pursuant to the FOIA.[2] Yet the agency has failed to fulfill its commitment more than six months later.

Instead, the agency has made inconsistent and unsupported exemption claims in this case. First, the agency provided another final determination letter on December 16, 2025, again refusing to release any portion of the report and asserting that the entirety of each of the 111 pages was properly withheld under Exemption 5. Then, on February 11, 2026, two days before the government's Pre-Motion Statement was due, the agency emailed EPIC a "corrected" final determination that, for the first time, claimed the report was also being withheld under Exemptions 1,[3] 6, and 7(E) in addition to the previous Exemption 5 claim.

---

[1] https://www.nextgov.com/cybersecurity/2025/07/cisa-release-telecom-security-report-its-director-nominee-nears-confirmation/407063/. Two days before Defendant filed its Pre-Motion Statement, the agency sent Plaintiff a "Corrected" Final Response letter (attached as "Exhibit A") that newly invoked the b1 exemption, although this did not appear in Defendant's Pre-Motion Statement. There was no prior indication that Defendant's "Final" Response Letter of 45 days prior was not, in fact, final. Even if the government had raised the b1 exemption, such arguments have been rightly described as "frankly absurd." https://www.congress.gov/congressional-record/volume-172/issue-23/senate-section/article/S438-2?q=%7B%22search%22%3A%22cyber%22%7D&s=4&r=1 ("In that call, Dr. Gottumukkala made a new claim that releasing the report would threaten our country's cyber security. Given that the report details vulnerabilities that are already actively being exploited by our adversaries and urgently need to be remediated, Dr. Gottumukkala's claim is frankly absurd.").

[2] EPIC is willing to introduce evidence to support this assertion, if such evidence would be useful to the Court, through an appropriate process.

[3] The agency has not made any arguments in support of its supposed Exemption 1 claim in its Pre-Motion Statement.

The report at issue, "U.S. Telecommunications Insecurity 2022", was drafted by a third-party contractor to provide an assessment of and describe potential cybersecurity risks in America's communications networks. The report has been reviewed by numerous individuals across the government, including by Congressional staff, and has not been kept internal to CISA or limited to any identified deliberative process. Indeed, the agency has not even identified any category of decision to which this report could theoretically be considered deliberative. And the agency's public commitment to release the record undermines any claim that any deliberations would be harmed by its potential release.

On the other hand, the public interest in disclosure of this report is enormous. After reviewing the report, Senator Ron Wyden warned that in the wake of the massive and severe Salt Typhoon hack—the report "includes details that are relevant to policymakers and Americans who care about the security of their phones," Nomination of Sean Plankey, 171 Cong. Rec. Vol. 64 at S2508 (Apr. 9, 2025),[4] and that "the American people have a right to read this report and the shocking information it contains." Morning Business, 172 Cong. Rec. Vol. 23 at S439 (Feb. 2, 2026).[5] And Congress continues to investigate vulnerabilities in our networks and to evaluate the proper legislative response to these significant risks. *See, e.g.*, "Safeguarding Americans' Communications: Strengthening Cybersecurity in a Digital Era", Hearing Before the Subcomm. on Commc'ns and Tech. 118th Cong. (Jan. 9, 2024).[6]

[4] https://www.congress.gov/congressional-record/volume-171/issue-64/senate-section/article/S2508-2.
[5] https://www.congress.gov/congressional-record/volume-172/issue-23/senate-section/article/S438-2?q=%7B%22search%22%3A%22cyber%22%7D&s=4&r=1.
[6] https://energycommerce.house.gov/events/communications-and-technology-subcommittee-hearing-safeguarding-americans-communications-strengthening-cybersecurity-in-a-digital-era.

Plaintiff intends to oppose the anticipated motion for Summary Judgment by Defendant, Cybersecurity and Infrastructure Security Agency (CISA), and intends to file a cross-motion for Summary Judgment seeking an order for disclosure of the full report.

ARGUMENT

Congress enacted the FOIA with a strong policy in favor of disclosure—exemptions to release should be narrowly construed, and it is the government's burden to prove them. *See, e.g.*, *Petroleum Info. Corp. v. U.S. Dep't of Interior*, 976 F.2d 1429, 1434 (D.C. Cir. 1992) (citing *EPA v. Mink*, 410 U.S. 73, 87 (1973)); *id.* at 1439 (citing *DOJ v. Julian,* 486 U.S. 1, 8 (1988)); *Oglesby v. U.S. Dep't of Army*, 920 F.2d 57, 68 (D.C. Cir. 1990). In this instance, the government has not met its burden of proof because it has not established facts that support its exemption claims. Therefore, summary judgment in favor of the Plaintiff, EPIC, is appropriate.

Exemption 5 is inapplicable; and even if it were applicable, segregable material must be released.

To prove that the deliberative process exemption applies, the government must show that the document was pre-decisional and was part of a give-and-take deliberative process. *See, e.g.*, *Morley v. CIA*, 508 F.3d 1108, 1127 (D.C. Cir. 2007). To be considered part of a deliberative process, the agency must not only describe the process involved and the role played by the document in the course of that process (including its function and significance), but also must describe the nature of the decisionmaking authority vested in the office or person issuing the disputed documents and the positions of the author and recipient in the chain of command. *See, e.g.*, *Natl. Sec. Counselors v. CIA*, 960 F. Supp. 2d 101, 188 (D.D.C. 2013) (citing to *Elec. Frontier Found. v. DOJ*, 826 F.Supp.2d 157, 168 (D.D.C. 2011)). As in CISA's response letters to EPIC's Appeal, in its Pre-Motion Statement CISA still has not identified any decision or deliberation to which this report was necessary, nor any relevant legal authority.

To the extent that a document is both pre-decisional *and* part of a deliberative process *at all*, the agency must still perform a segregability analysis—a casual boilerplate statement will not suffice. *See, e.g.*, *Reps. Comm. for Freedom of the Press v. FBI*, 3 F.4th 350, 371–72 (D.C. Cir. 2021); *Loving v. Dep't of Def.*, 550 F.3d 32, 38 (D.C. Cir. 2008). Here the agency has not offered any evidence to support the conclusion that the entirety of this 111-page report lacks reasonably segregable material.

Exemption 5 is meant to protect internal deliberation within government agencies; allegations of harm must pertain to how disclosure "would" (not merely "could") diminish candor within the agency and explicitly requires focused and concrete demonstrations of why disclosure would impede agency deliberations going forward. *See, e.g.*, *Reps. Comm. for Freedom of the Press* at 369–70; *Petroleum Info. Corp. v. U.S. Dep't of Interior* at 1435. Exemption 5 protects opinions moreso than facts. *See, e.g., Natl. Ass'n of Home Builders v. Norton*, 309 F.3d 26, 39 (D.C. Cir. 2002); *Pub. Citizen v. OMB*, 598 F.3d 865, 876 (D.C. Cir. 2010) (quoting *In re Sealed Case,* 121 F.3d 729, 737 (D.C. Cir. 1997)).

Here, the agency has done nothing more than restate the legal standard for Exemption 5. The agency has not identified any concrete harm to a deliberative process that would stem from releasing this report. *See* DOJ Pre-Motion Statement (ECF No. 15) at 3-4 ["DOJ Statement"]. And what harm could possibly result? The agency has made numerous public statements about the report and about the cybersecurity vulnerabilities that the report analyzes. Indeed, the agency's derogatory statements about the report in its Pre-Motion Statement—for example, failing to present "supporting information necessary to verify the claims", DOJ Statement at 5—only heighten the public interest in reviewing the report. If there are unanswered questions about the nature of these vulnerabilities then surely the public's interest is best served by promoting

further research and analysis in public. The fact that the agency states now, definitively, that it made no decision based on the information contained within the report, DOJ Statement at 5, only further undermines its Exemption 5 claim. The agency has not answered any of the necessary questions to establish an Exemption 5 claim because it has not identified any specific deliberative process or decision to which the report was pre-decisional. *See Citizens for Resp. & Ethics in Washington v. DOJ*, 45 F.4th 963, 972 (D.C. Cir. 2022) (citing *Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 868 (D.C. Cir. 1980)); *see also Natl. Sec. Counselors* at 188.

To the extent Exemption 5 applies at all, the segregable portions of a document must still be released. The government strains credulity to say that every word on every page of the 111-page report is deliberative and pre-decisional. *See, e.g.*, *2024-NFPO-00295* Final Response Letter from Gregory Bridges at 1 (Nov. 19, 2024); *Case No: 1:25-cv-01765 Final Response* from Eric A. Neuschaefer at 1 (Dec. 16, 2025). Moreover, as a matter of law, the agency cannot prevail on a mere assertion that it "has conducted this segregability analysis and determined that the report merits withholding in full." DOJ Statement at 3.[7] *See also Milton v. DOJ*, 873 F. Supp. 2d 55, 59-60 (D.D.C. 2011) (quoting *Mead Data* at 251). Additionally, this kind of unsubstantiated conclusory statement flies in the face of a witness claiming that the document contains facts and policy recommendations that are not specific to the agency:

> "based on my staff's review of this report, this report is a technical document containing factual information about U.S. telecom security. Although the report includes some general recommendations, the report does not recommend or discuss specific policy options that CISA itself could take to address this threat. And I want to emphasize that this report contains important factual information that the public has a right to see. CISA must drop its purported 'deliberative process privilege' claim and stop hiding this important information from the public."

[7] DOJ has not responded to this segregability issue since EPIC first raised it in our Dec. 2024 appeal of the agency's categorical denial of the entirety of every page of the report in Nov. 2024.

Morning Business, 172 Cong. Rec. Vol. 23 at S439 (Feb. 2, 2026). If even only a small portion of the report contains what Senator Wyden has alleged, that portion must be released.

Exemption 7(E) is not applicable.

Exemptions 7(E) and 6 were newly raised as of two weeks ago, but neither are applicable in this case. Exemption 7(E) only applies to documents compiled for law enforcement purposes and "only to the extent that the production of such law enforcement records or information" would disclose law enforcement investigative techniques. 5 U.S.C. § 552(b)(7)(E). This report was not created for a law enforcement purpose, and moreover was not even commissioned by a law enforcement agency. This exemption cannot apply to a technical report that explains how deficient telecom cybersecurity practices have resulted in exploitable and exploited vulnerabilities.

As a threshold matter, this report was not compiled for law enforcement purposes. As DOJ has conceded, the report purports to: "identify specific threats to infrastructure in the communications sector, identify specific entities that are vulnerable to those threats, and mak[e] recommendations to mitigate those threats." DOJ Statement at 1-2. It was compiled by the contractor of a non-law enforcement agency to assess cybersecurity risks. DOJ describes CISA as an agency tasked with providing "specialized sector-specific expertise to critical infrastructure owners and operators", not law enforcement. DOJ Statement at 1. CISA describes its own responsibilities as limited to supporting, coordinating, and assessing cybersecurity issues,[8] not law enforcement. Indeed, the agency's Chief Counsel, Daniel Sutherland, described the agency in 2019 explicitly as "non-law enforcement." McGuireWoods LLP, *A Different Type of Federal*

[8] https://www.cisa.gov/resources-tools/resources/cisa-fact-sheet.

Agency: How DHS's Newest Cybersecurity Agency Can Help Your Business (Apr. 18, 2019).[9] Simply put, CISA is not a law enforcement agency, does not enforce civil or criminal laws, and therefore the report could not have been "compiled for adjudicative or enforcement purposes." *Stern v. FBI*, 737 F.2d 84, 88–899 (D.C. Cir. 1984).

Even if somehow this report could be construed as being compiled for a law enforcement purpose, release would not disclose the investigative techniques, procedures, or guidelines protected by Exemption 7(E) because the report is about U.S. telecom security, not law enforcement techniques, procedures, or guidelines. To the extent that such things are discussed in the report, those portions can be segregated or be subject to in-camera review. *See, e.g.*, *Elliott v. U.S. Dep't of Agric.*, 596 F.3d 842, 851 (D.C. Cir. 2010).

Exemption 6 does not apply when public interest outweighs privacy interest.

When the government adequately invokes Exemption 6, the court must balance the privacy interest at risk in disclosure against any public interest in the requested information. *See Multi Ag Media LLC v. Dep't of Agric.*, 515 F.3d 1224, 1228 (D.C. Cir. 2008). A privacy interest may be substantial and yet insufficient to overcome the public interest in disclosure, *see id.* at 1230 (citing to *Natl. Ass'n of Home Builders* at 35); *see also Prison Legal News v. Samuels*, 787 F.3d 1142, 1147 (D.C. Cir. 2015), especially where the disclosure relates to an agency's performance of its statutory duties and would "contribute significantly to public understanding of the operations or activities of the government." *Natl. Ass'n of Home Builders* at 33–36. The public interest in the security and privacy of all of our communications outweighs the privacy concerns of individuals associated with communications infrastructure companies, DOJ Statement at 8—especially where a Senator whose staff has reviewed the report has alleged a

[9] https://www.passwordprotectedlaw.com/2019/04/cisa-can-help-your-business/.

cover-up, and against the backdrop of a dire and still-worsening national cybersecurity posture. *See, e.g.*, Stephanie K. Pell, *Why dismantling the PCLOB and CSRB threatens privacy and national security*, Brookings (Feb. 18, 2025)[10]; Tim Starks, *US 'slipping' on cybersecurity, annual Cyberspace Solarium Commission report concludes*, CyberScoop (Oct. 22, 2025)[11]; Tim Starks, *Across party lines and industry, the verdict is the same: CISA is in trouble*, CyberScoop (Feb. 25, 2026).[12] The public has a right to know who has been negligent about the cybersecurity of their communications and of their mobile location data.

To the extent that there is any privacy interest at stake in this cybersecurity vulnerability report, it would be as to the names of specific private individuals (not corporations) contained in the report. But the agency has not identified any such information with specificity, and even if it could the remedy would simply be to redact those particular names in the version processed for disclosure. Here, the public interest in the privacy and security of our country's communications network, including what the government is "up to" in maintaining (or failing to maintain) that privacy and security clearly dominate and the Court should order disclosure with minimal, if any, redactions of specific names.

CONCLUSION

The government has failed to meet its burden to provide facts sufficient to show that the unclassified report at issue was pre-decisional and deliberate. It failed to show that CISA is a law enforcement agency, that the report was created for a law enforcement purpose, or that the report reveals law enforcement investigative techniques. It failed to adequately argue that the narrow exemptions to FOIA's disclosure mandate should apply here, especially in the agency's failure to

[10] https://www.brookings.edu/articles/why-dismantling-the-pclob-and-csrb-threatens-privacy-and-national-security/.
[11] https://cyberscoop.com/cyberspace-solarium-commission-report-budget-workforce-cuts/.
[12] https://cyberscoop.com/cisa-personnel-cuts-trump-second-term-analysis/.

perform an adequate segregability analysis. Given DHS's fundamental segregability failure resulting in additional, unnecessary litigation, its claiming foreseeable harm despite public commitments of release and having already processed the report for FOIA release, and its eleventh hour attempt to change the document's classified status, we ask the court to consider whether the FOIA gamesmanship that appears to have taken place here warrants sanctions for bad faith compliance with FOIA. *See, e.g.*, 5 U.S.C. § 552(a)(4)(F)(i) and (4)(G).

Respectfully submitted,

ALAN BUTLER, D.C. Bar #1012128
EPIC President and Executive Director

Jeramie D. Scott, D.C. Bar # 1025909
EPIC Senior Counsel

/s/ Christopher Frascella
Christopher Frascella, D.C. Bar # 1780901
EPIC Counsel

ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Avenue NW
Washington, D.C. 20036
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Dated: Feb. 27, 2026