IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W., Suite 200
Washington, D.C. 20009,

Plaintiff,

v.

UNITED STATES DEPARTMENT OF HOMELAND SECURITY,
Washington, D.C. 20528

Defendant.

Civ. Action No. 17-2047

COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, for injunctive and other appropriate relief to secure the release of agency records requested by Plaintiff Electronic Privacy Information Center ("EPIC") from Defendant National Protection and Programs Directorate ("NPPD") of the U.S. Department of Homeland Security ("DHS").

2. EPIC challenges the DHS's failure to make a timely decision concerning EPIC's request for records of DHS's research, integration, analysis, and other activities related to the Russian interference in the 2016 Presidential election, as well as the agency's failure to release any responsive records. EPIC seeks injunctive and other appropriate relief.

Jurisdiction and Venue

3. This Court has both subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 and 5 U.S.C. §§ 552(a)(6)(E)(iii) and 552(a)(4)(B). This Court has personal jurisdiction over Defendant DHS.

4. Venue is proper in this district under 5 U.S.C. § 552(a)(4)(B).

Parties

5. Plaintiff EPIC is a nonprofit organization, incorporated in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC's mission is oversight and analysis of government activities. EPIC's Advisory Board includes distinguished experts in law, technology, public policy, and cybersecurity. EPIC routinely disseminates information to the public through the EPIC website, the EPIC Alert, and various other news organizations. EPIC is a representative of the news media. *EPIC v. Dep't of Def.*, 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

6. Defendant DHS is a federal agency within the meaning of the FOIA, 5 U.S.C. § 552(f)(1). Defendant DHS is headquartered in Washington, D.C.

Facts

DHS Review of Russian Interference with the 2016 Presidential Election

7. The U.S. Intelligence Community ("IC") has concluded that Russia carried out a multi-pronged campaign to interfere in the 2016 U.S. Presidential Election to "undermine public faith in the US democratic process," demonstrating a "significant escalation" in Russian activities.[1] Nine months since the IC report on the interference, few new details of the interference have been made public.

8. The mission of the DHS is to "safeguard the American people, our homeland, and our values,"[2] and the agency accordingly has a key role in the federal response to Russian interference. On December 29, 2016, DHS and the Federal Bureau of Investigation published the

[1] Office of the Dir. of Nat'l Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections* ii (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.
[2] *Mission*, DHS.gov https://www.dhs.gov/mission (last visited July 10, 2017).

first public report on the interference — the "Joint Analysis Report," or JAR.[3] 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 services. While "[p]revious JARs have not attributed malicious cyber activity to specific countries or threat actors," the report stated, this report immediately identified "Russian civilian and military intelligence Services (RIS)" as the actors who "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."[4]

9. On January 6, 2017, then DHS Secretary Jeh Johnson announced the designation of election infrastructure as a subsector of the Government's critical infrastructure.[5] 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.[6]

10. Since the publication of the JAR and the critical infrastructure designation, DHS has continued the Russian interference investigation. But the agency has not provided any significant, new information to the American public.

---

[3] Dep't of Homeland Sec. & Fed. Bureau of Investigation. *GRIZZLY STEPPE – Russian Malicious Cyber Activity* (2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

[4] *Id*. at 1.

[5] Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (Jan. 6, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

[6] *Russian Interference in the 2016 U.S. Elections: Hearing Before H. Select Comm. on Intelligence*, 115th Cong. (2017), [hereinafter *Russian Interference Hearing Before H. Select Comm.*] https://intelligence.house.gov/uploadedfiles/jeh_johnson_-_prepared_statement_to_hpsci_-_6-21-17_hearing.pdf (written opening statement of Jeh Johnson, former Secretary, Department of Homeland Security).

11. In June 2017, the National Security Agency identified a Russian cyberattack that impacted at least one U.S. voting software supplier and Russian agents sent spear-phishing emails to more than one hundred local election officials before Election Day 2016.[7] It was reported that Neither the software supplier, VR Systems, nor local officials were warned before Election Day that Russian hackers could have compromised their software.[8] Notably, North Carolina investigated whether any local systems were breached after complaints coming from Durham reported problems involving electronic poll books supplied by VR Systems.[9] While there is no evidence the two incidents are linked, there is evidence that there are gaps in our Government's efforts to secure elections.[10]

12. On June 21, 2017, nearly eight months after election day, in an open hearing before the Senate Select Committee on Intelligence, NPPD's Acting Deputy Under Secretary for Cybersecurity and Communications Jeanette Manfra confirmed for the first time that "election-related systems in 21 states were targeted" by Russian cyber actors during the 2016 election cycle.[11] Nearly *half of the United States* were targets of Russian activities during the 2016

---

[7] Matthew Cole et. al., *Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election*, The Intercept (June 5, 2017, 3:44 PM), https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.

[8] Nicole Perlroth et. al., *Russian Election Hacking Efforts, Wider than Previously Known, Draw Little Scrutiny*, N.Y. Times (Sept. 1, 2017), https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html?mcubz=0.

[9] *Id*.

[10] Pam Fessler, *Russian Cyberattack Targeted Elections Vendor Tied to Voting Day Disruptions*, NPR (Aug. 10, 2017, 3:47 PM), http://www.npr.org/2017/08/10/542634370/russian-cyberattack-targeted-elections-vendor-tied-to-voting-day-disruptions?utm_campaign=storyshare&utm_source=twitter.com&utm_medium=social.

[11] *Russian Interference in the 2016 U.S. Elections: Hearing Before S. Select Comm. on Intelligence*, 115th Cong. (2017), https://www.intelligence.senate.gov/hearings/open-hearing-russian-interference-2016-us-elections (testimony of Jeanette Manfra, Acting Deputy Under Secretary, Department of Homeland Security).

election cycle.[12] Acting Deputy Under Secretary Manfra did not indicate which states were affected. When pressed to disclose the states from which data was exfiltrated, Ms. Manfra stated, "I prefer not to go to those details in this forum, Sir."[13]

13. Vice Chair Mark Warner (D-VA) questioned Ms. Manfra during the hearing about whether "at this moment in time there may be a number of state and local election officials that don't know their states were targeted in 2016."[14] Senator Rubio (R-FL) urged, "[A]s much of [the systems data] must be made available to the public as possible," and said to "err on the side of disclosure about our systems so people have full confidence when they go vote."[15] Special elections for both House and Senate seats are scheduled for the winter of 2017.

14. Former DHS Secretary Johnson emphasized in written testimony to the House Select Committee on Intelligence on June, 21, 2017, that his "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 strengthen our cybersecurity generally, and the cybersecurity around our political/election process specifically."[16] He indicated that he 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."[17]

---

[12] *Id*.
[13] *Id*.
[14] *Id*.
[15] *Id*.
[16] *Russian Interference Hearing before H. Select Comm.*, *supra* note 6 (written opening statement of Jeh Johnson, former Secretary, Department of Homeland Security).
[17] *Id*.

15. Following the abrupt cancellation of a critical House Select Intelligence Committee public hearing on the Russian interference [18] scheduled on March 28, 2017, Ranking member Bennie Thompson (D-MS) introduced House Resolution 235.[19] The Resolution directed the Secretary of Homeland Security to transmit directly to the House of Representatives DHS's research, integration, analysis, and other documentation of its investigation of the Russian interference.[20]

16. On March 31, 2017, EPIC filed a FOIA request with the Department of Homeland Security, described in more detail below, seeking the records described in House Resolution 235.

17. On September 13, 2017, Acting Secretary of Homeland Security Elain Duke issued a Binding Operational Directive to Federal Executive Branch departments and agencies to stop using software made by the Russian cybersecurity firm Kasperksy Lab.[21] In a statement, DHS said "[t]he risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security."[22]

18. There is a profound and urgent public interest in the release of records in possession of the DHS sought by EPIC concerning the Russian interference with the 2016 Presidential Election. The release of these records is necessary for the public to evaluate DHS's response to the Russian interference, assess future threats to American democratic institutions, and to ensure

---

[18] Patricia Zengerle, *House Intelligence Panel Leaders Split Over Session on Russia*, Reuters (Mar. 24, 2017, 12:44 PM), http://www.reuters.com/article/us-usa-trump-russia-idUSKBN16V29I (Reporting that House Intelligence Committee Chairman Devin Nunes cancelled the Tuesday public hearing on the previous Friday).

[19] H. Res. 235, 115th Cong. (2017).

[20] *Id.*

[21] DHS Statement on the Issuance of Binding Operational Directive 17-01 (Sept. 13, 2017), https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01.

[22] *Id*.

the accountability of the federal agency with the legal authority to safeguard the American people against foreign cyber-attacks.

EPIC's FOIA Request

19. On March 31, 2017, EPIC submitted a FOIA request ("EPIC's FOIA Request") to the U.S. Department of Homeland Security ("DHS"). The FOIA request was transferred to DHS's National Protection and Programs Directorate ("NPPD") for direct response.

20. EPIC's FOIA Request sought records based on H.R. 235. 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 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.

21. EPIC sought "news media" fee status under 5 U.S.C. § 552(4)(A)(ii)(II) and a waiver of all duplication fees under 5 U.S.C. § 552(a)(4)(A)(iii).

22. EPIC also sought expedited processing under 5 U.S.C. § 552(a)(6)(E)(v)(II).

23. In an e-mail dated May 10, 2017, NPPD FOIA Office acknowledged receipt of EPIC's FOIA Request. The request was assigned reference number 2017-NPFO-00430. The NPPD stated the "perfected request was . . . transferred to DHS's National Protection and Programs Directorate on April 14, 2017, for direct response to [EPIC]." The NPPD did not include any decision concerning EPIC's request for mews media status, fee waiver, or expedited processing.

EPIC's Constructive Exhaustion of Administrative Remedies

24. Today is the 188th day since DHS component NPPD received EPIC's FOIA Request.

25. The DHS has failed to make a determination regarding EPIC's request for expedited processing within the time period prescribed by 5 U.S.C. § 552(a)(6)(E)(ii)(I).

26. Additionally, the DHS has failed to make a determination regarding EPIC's FOIA Request within the time period required by 5 U.S.C. § 552(a)(6)(A)(ii).

27. EPIC has exhausted all administrative remedies under 5 U.S.C. § 552(a)(6)(C)(i).

Count I

Violation of FOIA: Failure to Comply with Statutory Deadlines

28. Plaintiff asserts and incorporates by reference paragraphs 1–26.

29. Defendant DHS has failed to make both a determination regarding EPIC's request for expedited processing and a determination regarding EPIC's FOIA request for 188 days and has thus violated the deadlines under 5 U.S.C. §§ 552(a)(6)(E)(ii)(I), (a)(6)(A)(ii).

30. Plaintiff has constructively exhausted all applicable administrative remedies under 5 U.S.C. § 552(a)(6)(C)(i).

Count II

Violation of FOIA: Failure to Grant Request for Expedited Processing

31. Plaintiff asserts and incorporates by reference paragraphs 1–26.

32. Defendant's failure to grant plaintiff's request for expedited processing violated the FOIA, 5 U.S.C. § 552(a)(6)(E)(i).

33. Plaintiff is entitled to injunctive relief with respect to an agency determination on EPIC's request for expedited processing.

Count III

Violation of FOIA: Unlawful Withholding of Agency Records

34. Plaintiff asserts and incorporates by reference paragraphs 1–26.

35. Defendant DHS has wrongfully withheld agency records requested by Plaintiff.

36. Plaintiff has exhausted all applicable administrative remedies under 5 U.S.C. § 552(a)(6)(C)(i).

37. Plaintiff is entitled to injunctive relief with respect to the release and disclosure of the requested records.

Requested Relief

WHEREFORE, Plaintiff requests that this Court:

A. Order Defendant to immediately conduct a reasonable search for all responsive records;

B. Order Defendant to take all reasonable steps to release nonexempt records;

C. Order Defendant to disclose to Plaintiff all responsive, non-exempt records;

D. Order Defendant to produce the records sought without the assessment of search fees;

E. Order Defendant to grant EPIC's request for a fee waiver;

F. Award EPIC costs and reasonable attorney's fees incurred in this action; and

G. Grant such other relief as the Court may deem just and proper.

Respectfully Submitted,

/s/ Alan Butler

Alan Butler, D.C. Bar # 1012128
EPIC Senior Counsel

Marc Rotenberg, D.C. Bar # 422825
EPIC President and Executive Director

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Dated: October 4, 2017