epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

June 20, 2017

The Honorable Richard Burr, Chair
The Honorable Mark Warner, Ranking Member
U.S. Senate Select Committee on Intelligence
211 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Burr and Ranking Member Warner:

In advance of the hearing on "Russian Interference in the 2016 U.S. Elections,[1]" we write to you again regarding EPIC's interest in the challenge of protecting democratic institutions against foreign adversaries and cyber attack. [2] The Electronic Privacy Information Center ("EPIC") is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[3] EPIC is a leading advocate for civil liberties and democratic values in the information age, and works closely with a distinguished Advisory Board, with specific expertise in cyber security and voting technology.[4]

After reports emerged about Russian interference with the 2016 election, EPIC launched a new project on Democracy and Cybersecurity.[5] EPIC is currently pursuing four Freedom of Information Act matters to learn more about the Russian interference in the 2016 Presidential election.[6] EPIC is pursing these matters because, as we stated recently *The Hill*,

> The public has a right to know the details when a foreign government attempts to influence the outcome of a U.S. presidential election. The public has a right to know the extent of the risk and how the government agencies, tasked with

[1] *Russian Interference in the 2016 U.S. Elections,* 115th Cong. (2017), S. Select Comm. on Intelligence, https://www.intelligence.senate.gov/hearings/open-hearing-russian-interference-2016-us-elections (June 21, 2017).
[2] Letter from EPIC to Senator Richard Burr and Senator Mark Warner, S. Select Comm. on Intelligence (Mar. 29, 2017), *available at* https://epic.org/testimony/congress/EPIC-SSCI-Russia-Mar2017.pdf.
[3] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[4] *See* EPIC Advisory Board, https://epic.org/epic/advisory_board.html. *See, e.g.,* Douglas Jones and Barbara Simons, Broken Ballots: Will Your Vote Count? (2012); Ron Rivest and Phil Stark, *Still Time for an Election Audit,* USA Today, Nov. 18, 2016.
[5] *See* EPIC, *Democracy and Cybersecurity: Preserving Democratic Institutions*, https://epic.org/democracy/.
[6] *EPIC v. ODNI*, No. 17-163 (D.D.C. filed Jan. 25, 2017); *EPIC v. FBI*, No. 17-121 (D.D.C. filed Jan. 18, 2017); *EPIC Seeks Release of FISA Order for Trump Tower*, EPIC (March 6, 2017), https://epic.org/2017/03/epic-seeks-release-of-fisa-ord.html; *EPIC v. IRS*, No. 17-670 (D.D.C. filed Apr. 15, 2017).

defending the nation, responded. And the public has a right to know what steps have been taken to prevent future attacks.[7]

In *EPIC v. ODNI*, EPIC is seeking the release of the complete intelligence report on the Russian interference with the 2016 election. A limited, declassified version of the report was published on Jan. 6, 2017.[8] This report stated that Russia carried out a multi-pronged attack on the 2016 U.S. Presidential Election to "undermine public faith in the US democratic process." The report also states that "this version does not include the full supporting information on key elements of the influence campaign."

There is an urgent need to make available to the public the Complete ODNI Assessment to fully assess the Russian interference with the 2016 Presidential election and to prevent future attacks on democratic institutions.[9] The Declassified ODNI Assessment failed to provide critical information about the extent and nature of the Russian interference and leaves significant questions unanswered. For example, while the report notes that "Russian actors" had been "targeting or compromising" democratic institutions including "state or local election boards" since "early 2014," the report provides no further detail on these intrusions or the extent of the damage or future threats involved. The Declassified ODNI Assessment also did not identify which systems in the United States were attacked, whether voter records of Americans were obtained, the ongoing risks to U.S. political parties and other democratic institutions, or whether similar activities could impact democratic institutions in other countries.

The Director of National Intelligence recently provided a "non-responsive response" to EPIC. The intelligence agency was required to release all "non-exempt portions" of the report to EPIC on May 3, 2017. However, the agency withheld the entire document, refusing to provide even partial information that should have been released to EPIC under the Freedom of Information Act.[10] EPIC will challenge the agency's response as the litigation continues in federal district court in Washington, DC.

In *EPIC v. FBI*, EPIC seeks to understand the FBI's response to the Russian interference in the 2016 Presidential election. The FBI is the lead federal agency for investigating cyber attacks in the United States by criminals, overseas adversaries, and terrorists."[11] Nonetheless, questions were raised about the failure of the FBI to adequately investigate the attacks on the nation's political institutions.[12] EPIC is therefore pursuing FBI records to help the "public. . . . evaluate

---

[7] Marc Rotenberg, *Americans have a right to know what intel community knows on Russia*, The Hill (March 27, 2017).

[8] Office of the Dir. of Nat'l Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections* (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf [hereinafter Declassified ODNI Assessment].

[9] Complaint at 3, *EPIC v. ODNI*, *supra* note 5.

[10] 5 U.S.C. 552(a)(8)(A)(ii).

[11] *What We Investigate, Cyber Crime*, FBI.gov, https://www.fbi.gov/investigate/cyber; Directive on United States Cyber Incident Coordination ("PPD 41"), 2016 Daily Comp. Pres. Doc. 495 (July 26, 2016) (setting forth the FBI's legal authority for cybersecurity threat response).

[12] Ellen Nakashima & Adam Entous, *FBI and CIA Give Differing Accounts to Lawmakers on Russia's Motives in 2016 Hacks*, Wash. Post (Dec. 10, 2016), https://www.washingtonpost.com/world/national-security/fbi-and-cia-give-differing-accounts-to- lawmakers-on-russias-motives-in-2016-

the FBI response to the Russian interference, assess threats to American democratic institutions, and to ensure the accountability of the federal agency with the legal authority to safeguard the American people against foreign cyber attacks."[13]

EPIC has now obtained the document set regarding FBI procedures for notifying victims of cyberattacks. According to the procedure for "Victim Notification in Computer Intrusion Matters" in the FBI Cyber Division (CyD) Policy Guide (emphasis added):

> CyD's top priority is the protection of our national security, economy, and information infrastructure from intrusions, malicious code, and nefarious computer network operations. This effort entails the sharing of investigative information with intrusion victims and the CND community to protect compromised systems, mitigate economic loss and damage, and prevent future attacks. Victim notification is a compelling way for CyD to contribute to network defense for the protection of individual, commercial, and government users of the Internet, as well as for the protection of the infrastructure itself. It is the policy of CyD to notify and disseminate meaningful information to victims and the CND community in a timely manner to the extent to which it does not interfere with ongoing law enforcement or USIC investigations, operations, methods, sources, or technologies.
>
> In a computer intrusion investigation, the victim to be notified is the individual, organization, or corporation that is the owner or operator of the computer at the point of compromise or intrusion. Cyber victims are generally individuals or organizations subjected to cyber-based operations, including computer network attack (CNA) and computer network exploitation (CNE), in furtherance of criminal activity or threats to national security. These CNA and CNE operations often result in the compromise of electronic systems, resulting in the alteration, loss, exfiltration, or denial of access to data that the victim maintains or controls. Victims may be identified, to the extent possible, by the FBI or its partner agencies in the course of investigative activities of suspected cybercrimes and cyber-related threats.
>
> Because timely victim notification has the potential to completely mitigate ongoing and future intrusions and can mitigate the damage of past attacks while increasing the potential for the collection of actionable intelligence, CyD's policy regarding victim notification is designed to strongly favor victim notification. Even when it may interfere with another investigation or USIC operation, notification should still be considered in coordination with the operational stakeholders when the equities of victim notification serve to protect USPERs, a national infrastructure, or other U.S. interests from significant harm.[14]

---

hacks/2016/12/10/c6dfadfa-bef0-11e6-94ac- 3d324840106c_story.html.

[13] Complaint at 7, *EPIC v. FBI*, *supra* note 5.

[14] Cyber Division Policy Guide at 4.7, *available at* https://epic.org/foia/fbi/russian-hacking/EPIC-16-12-22-FBI-FOIA-20170511-Production-2.pdf.

As you aware, the Intelligence community assessed that both the DNC and the RNC were subject to a cyber attack by the Russian government.[15] The obvious question at this point is whether the FBI followed the required procedures for Victim Notification once the Bureau became aware of this attack. EPIC urges the Committee to explore the following questions with the FBI witness:

- **Did the FBI follow the procedures set forth in the "Victim Notification in Computer Intrusion Matters" Policy Guide and notify the DNC and the RNC once it became aware of the Russian cyberattack?**

- **Does the Policy Guide establish adequate procedures for cyber attacks on US political organizations or should new policies be adopted?**

- **Did the FBI do all it should have done to alert the DNC and the RNC once it learned about cyber attacks?**

- **Should the United States be concerned about future cyber attacks that could destabilize our democratic institutions?**

The urgency of understanding the full scope of the Russian threat to democratic elections is clear. There are upcoming federal elections in Europe. The German national election is September 24, 2017. National elections will also take place in Italy and Austria this fall. Russian attacks on democratic institutions are expected to continue.[16] The U.S. Intelligence community has reportedly shared the classified ODNI report with European governments to help limit Russian interference with their elections.[17] The public has "the right to know" the extent of Russian interference with democratic elections and the steps that are being taken to prevent future attacks.[18] The need to understand Russian efforts to influence democratic elections cannot be overstated.

We ask that this Statement from EPIC be entered in the hearing record. EPIC will keep the Committee apprised of the documents we receive in our FOIA cases. We look forward to working with you on the cybersecurity risks to democratic institutions.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

---

[15] Office of the Dir. of Nat'l Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections* (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf [hereinafter Declassified ODNI Assessment].
[16] Declassified ODNI Assessment, *supra* note 7, at 5.
[17] Martin Matishak, *U.S. shares hacking intel with Europe as Russia shifts focus*, POLITICO Pro (Feb. 6, 2017).
[18] "A people who mean to be their own Governors must arm themselves with the power knowledge gives," James Madison. *See generally* EPIC, *Open Government*, https://epic.org/open_gov/.