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 7, 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

RE: Open Hearing: Former FBI Director James Comey

Dear Chairman Burr and Ranking Member Warner:

In advance of the hearing with former FBI Director James Comey,[1]" we write to you regarding the FBI's response to Russian interference in the 2016 Presidential Election. EPIC is currently pursuing a Freedom of Information Act case against the FBI, EPIC v. FBI,[2] to determine whether the FBI did all that it should have done when it became aware of foreign cyber attacks on US political institutions, including the DNC and the RNC.

The FBI is the lead federal agency for investigating cyber attacks by overseas adversaries, and terrorists."[3] Substantial questions were raised about the failure of the FBI to adequately investigate the attacks on the nation's political institutions.[4] EPIC is seeking to help the "public. . . . evaluate 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."[5] We are specifically seeking the public release of:

> (1) All records including, but not limited to, memos, reports, guidelines, procedures, summaries, and emails pertaining to the FBI's investigation of Russian-sponsored cyber attack on the RNC, DNC, and DCCC.

---

[1] *Former Director James Comey,* 115th Cong. (2017), S. Select Comm. on Intelligence, https://www.intelligence.senate.gov/hearings/open-hearing-former-director-james-comey-fbi (June 8, 2017).
[2] *EPIC v. FBI*, No. 17-121 (D.D.C. Filed Jan. 18, 2017).
[3] *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).
[4] 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-hacks/2016/12/10/c6dfadfa-bef0-11e6-94ac- 3d324840106c_story.html.
[5] Complaint at 7, *EPIC v. FBI*, *supra* note 5.

(2) All records of communications to the RNC, DNC, and DCCC regarding the threat of Russian interference in the 2016 Presidential election.
(3) All records of communications with other federal agencies regarding Russian interference in the 2016 Presidential election.

(4) All records including, but not limited to, memos, reports, guidelines, and procedures pertaining to the FBI's procedure to notify targets of cyber attacks.

EPIC has now obtained the document set regarding FBI procedures for notifying victims of cyberattacks (category 4 above). 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.[6]

As you aware, the Intelligence community assessed that both the DNC and the RNC were subject to a cyber attack by the Russian government.[7] 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 ask former Director Comey the following questions:

Mr. Comey – Did the FBI follow the procedures set forth in FBI Cyber Division's "Victim Notification in Computer Intrusion Matters" Policy Guide to notify the DNC and the RNC once it became aware of the Russian cyberattack on US political organizations?

Mr. Comey – Did the FBI do all it should have done to alert the DNC and the RNC once it learned about cyber attacks to their systems?

Mr. Comey - Should the United States be concerned that we could be subject to future cyber attacks that would destabilize our democratic institutions?

The urgency of understanding the full scope of the problem is clear. 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.[8] Mr. Comey, more than anyone, will know whether the Bureau responded effectively to the threat.

We appreciate that there will be considerable interest in the communications between Mr. Comey and the President regarding the investigation that followed. Nonetheless, we urge you to determine whether the FBI took the necessary steps prior to the election to respond to the Russian interference. On that issue as well, Mr. Comey is the key witness.

We ask that EPIC Statement be entered in the hearing record. EPIC will keep the Committee apprised of the documents we receive in our FOIA cases and 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

[6] 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.
[7] 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].
[8] "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/.