

CHARLES E. GRASSLEY, IOWA, CHAIRMAN

ORRIN G. HATCH, UTAH
JEFF SESSIONS, ALABAMA
LINDSEY O. GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
MICHAEL S. LEE, UTAH
TED CRUZ, TEXAS
JEFF FLAKE, ARIZONA
DAVID VITTER, LOUISIANA
DAVID A. PERDUE, GEORGIA
THOM TILLIS, NORTH CAROLINA

PATRICK J. LEAHY, VERMONT
DIANNE FEINSTEIN, CALIFORNIA
CHARLES E. SCHUMER, NEW YORK
RICHARD J. DURBIN, ILLINOIS
SHELDON WHITEHOUSE, RHODE ISLAND
AMY KLOBUCHAR, MINNESOTA
AL FRANKEN, MINNESOTA
CHRISTOPHER A. COONS, DELAWARE
RICHARD BLUMENTHAL, CONNECTICUT

United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

KOLAN L. DAVIS, Chief Counsel and Staff Director
KRISTINE J. LUCIUS, Democratic Chief Counsel and Staff Director

July 26, 2016

VIA ELECTRONIC TRANSMISSION

The Honorable Loretta Lynch
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

The Honorable James B. Comey, Jr.
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, DC 20535

Dear Attorney General Lynch and Director Comey:

We are writing in regard to the recent cyberattacks on American political organizations. Yesterday the FBI confirmed that it is investigating the recent hack of the Democratic National Committee (DNC). We are writing to request more specific information about the efforts that the National Cyber Investigative Joint Task Force (NCIJTF) and other elements of the FBI and Justice Department are undertaking in order to counter these types of attacks and bring the perpetrators to justice.

On June 14, 2016, the Washington Post reported that Russian government hackers had successfully penetrated the computer network of the Democratic National Committee, gaining access to DNC databases and email.¹ According to the article, DNC officials noticed unusual network activity and hired CrowdStrike, a cybersecurity firm, to investigate. The firm identified two separate groups of hackers who had penetrated the DNC network, both of which it determined were working for the Russian government. Immediately after the Washington Post report, a purported hacker calling himself “Guccifer 2.0” claimed responsibility for the hack, and further claimed to be a lone Romanian hacker.² The Russian government also denied its involvement.³ However, evidence appears to undermine the Romanian hacker’s claim of

¹ Ellen Nakashima, *Russian Government Hackers Penetrated DNC, Stole Opposition Research On Trump*, THE WASHINGTON POST, June 14, 2016.

² Lorenzo Franceschi-Bicchierai, *‘Guccifer 2.0’ Is Likely A Russian Government Attempt To Cover Up Their Own Hack*, MOTHERBOARD, June 16, 2016.

³ Andrew Roth, *Russia Denies DNC Hack And Says Maybe Someone ‘Forgot The Password,’* THE WASHINGTON POST, June 15, 2016.

responsibility and instead suggests the Russian government's involvement.⁴ The hackers subsequently publicly released what appears to be the DNC's opposition research on Donald Trump in June.⁵ Last week, WikiLeaks released roughly 20,000 of the hacked DNC emails that the hackers had provided to it.⁶

It is not unusual for a nation's intelligence services to obtain sensitive information from other nations' political entities. Not only has James Clapper, the Director of National Intelligence, stated that the government has indications of cyberattacks on the 2016 presidential campaigns, the government has also reported that foreign hackers targeted the networks of the Romney and Obama campaigns in 2012, and that Chinese hackers compromised the networks of the Obama and McCain campaigns in 2008.⁷

However, when a foreign intelligence service not only spies on American political organizations, which is bad enough, but then selectively publishes the obtained information in what appear to be attempts to affect our democratic process, it is substantially more troubling. The integrity of the democratic process is essential to the social contract on which our republic is formed. If foreign intelligence agencies are attempting to undermine that process, the U.S. government should treat such efforts even more seriously than standard espionage. These types of cyberattacks are significant and pernicious crimes. Our government must do all that it can to stop such attacks and to seek justice for the attacks that have already occurred.

We were pleased to see that the FBI has stated that it is investigating this situation. We are writing to request more information on this cyberattack in particular and more information in general on how the Justice Department, FBI, and NCIJTF attempt to prevent and punish these types of cyberattacks. Accordingly, please respond to the following by August 9, 2016:

1. When did the Department of Justice, FBI, and NCIJTF first learn of the DNC hack? Was the government aware of the intrusion prior to the media reporting it?
2. Has the FBI deployed its Cyber Action Team to determine who hacked the DNC?
3. Has the FBI determined whether the Russian government, or any other foreign government, was involved in the hack?
4. In general, what actions, if any, do the Justice Department, FBI, and NCIJTF take to prevent cyberattacks on non-governmental political organizations in the U.S.,

⁴ E.g., Dmitri Alperovitch, *Bears In The Midst: Intrusion Into The Democratic National Committee*, CROWDSTRIKE, June 15, 2016; Lorenzo Franceschi-Bicchierai, *We Spoke to DNC Hacker 'Guccifer 2.0.'* MOTHERBOARD, June 21, 2016; Eli Lake, *Cybersecurity Experts Say Russia Hacked The Democrats*, BLOOMBERG, July 25, 2016; Thomas Rid, *All Signs Point To Russia Being Behind The DNC Hack*, MOTHERBOARD, July 25, 2016; Evan Perez, *Russians Suspected Of Hacking Democratic National Committee Emails*, CNN, July 25, 2016.

⁵ Caitlin Yilek, *Stolen DNC Files On Trump Leaked*, THE HILL, June 15, 2016.

⁶ Andrea Peterson, *Wikileaks Post Nearly 20,000 Hacked DNC Emails Online*, THE WASHINGTON POST, July 22, 2016.

⁷ Ellen Nakashima, *National Intelligence Director: Hackers Have Targeted 2016 Presidential Campaigns*, THE WASHINGTON POST, May 18, 2016.

such as campaigns and political parties? Does the government consult or otherwise communicate with the organizations to inform them of potential threats, relay best practices, or inform them of detected cyber intrusions?

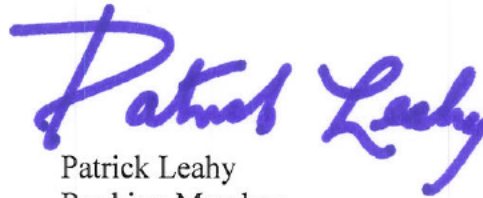
5. Does the Justice Department believe that existing statutes provide an adequate basis for addressing hacking crimes of this nature, in which foreign governments hack seemingly in order to affect our electoral processes?

In addition to the questions listed above, we also request that the Justice Department, FBI, and/or NCIJTF arrange a briefing on these issues for Committee staff by August 16, 2016. If possible, we also request that the briefing include a staff tour of NCIJTF's facilities. Thank you for your attention to this important matter. If you have any questions, please contact Patrick Davis of the Committee Staff at (202) 224-5225 or [REDACTED].

Sincerely,



Charles E. Grassley
Chairman
Senate Committee on the Judiciary



Patrick Leahy
Ranking Member
Senate Committee on the Judiciary

cc: The Honorable Donald Freese
Director
National Cyber Investigative Joint Task Force

The Honorable John P. Carlin
Assistant Attorney General
National Security Division
Department of Justice

The Honorable James C. Trainor, Jr.
Assistant Director
Cyber Division
Federal Bureau of Investigation