BOB GOODLATTE, Virginia
CHAIRMAN

JERROLD NADLER, New York
RANKING MINORITY MEMBER

U.S. House of Representatives
Committee on the Judiciary
Washington, DC 20515–6216
One Hundred Fifteenth Congress

February 8, 2018

The Honorable Bob Goodlatte
Chairman
House Judiciary Committee
2138 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Goodlatte:

We write to request that the Committee hold immediate hearings to examine vulnerabilities in our election infrastructure, threats posed to that infrastructure by foreign actors, and what steps the Trump Administration may or may not be taking to ensure the integrity of our state and federal elections. We believe the threat is urgent. The leadership of the Department of Justice, the Department of Homeland Security, and the Department of State should come before our Committee to inform us of their plans to protect the integrity of our election systems.

In February of 2017, you offered an amendment to our oversight plan that, as subsequently amended by Representative David Cicilline (D-RI), stated our intention to conduct oversight into allegations of foreign interference with federal elections.[1] Unfortunately, since then, we have not held a single hearing on the topic.

We have, however, heard alarming testimony on this front from the leadership of the Department of Justice and the FBI. Other high ranking Administration officials have also made similar statements. CIA Director Pompeo and Secretary of State Tillerson both recently confirmed that Russia is already targeting the 2018 elections. Yesterday, Jeanette Manfra, DHS's leading cybersecurity official, admitted that the Russian government penetrated our election systems in 2016.[2] Even former President George W. Bush has acknowledged that there is "pretty clear evidence that the Russians meddled" in the last election.[3]

---

[1] *Markup of Authorization and Oversight Plan; H.R. 985; H.R. 906*, before the H. Comm. on the Judiciary, Feb. 15, 2017 (statement of Chairman Robert Goodlatte).

[2] Doug Stanglin, *Russia already meddling in U.S. midterm elections, Tillerson says*, USA TODAY, Feb. 7, 2018; Cynthia McFadden et al., *Russians penetrated U.S. voter systems, says top U.S. official*, NBC, Feb. 7, 2018.

[3] Kim Hjelmgaard, *George W. Bush: "Clear Evidence Russians meddled" in election*, USA TODAY, Feb. 8, 2018.

To be clear, every official to speak on this topic so far—including Attorney General Jeff Sessions, Deputy Attorney General Rod Rosenstein, and FBI Director Christopher Wray—has stood by the intelligence community's January 2017 assessment that the Russian government interfered with the 2016 presidential election. The Department of Homeland Security has recognized the gravity of the threat and classified America's election infrastructure as critical infrastructure under the Critical Infrastructures Protection Act of 2001. The FBI has since created a "Foreign Influence Election Taskforce" to help prepare for any future attacks.

Unfortunately, the Department of Justice appears to have taken little—if any—action to secure our election systems going forward. When he appeared before our Committee, Attorney General Sessions was asked if the Department is at least reviewing the laws on the books to see what additional authority he might need to secure our election infrastructure. He gave a completely unsatisfactory answer: "We have discussed those matters, but no completion has been done. ... We are not anywhere near where I would like us to be, yet." He later agreed he had not, in fact, ordered any review of relevant federal law[4]—ignoring President Trump's executive order to strengthen federal networks and infrastructure.[5] Although the Attorney General promised our members a briefing on the topic, but that was more than nine weeks ago. The Department of Justice has not yet responded to the request we sent him on December 1, 2017.[6]

We cannot afford to ignore the mounting evidence of a coordinated effort to undermine the most basic and essential aspects of democratic process. In addition to the alarming disclosures that came to light this week:

- The Department of Homeland Security notified at least 21 states that the Russian government targeted and, in some cases, successfully penetrated their election infrastructure.[7]
- Illinois officials found 90,000 voter files were stolen—more than 75,000 containing personal data such as driver's license and social security numbers. Officials found evidence of an additional attempt to download the state's entire voter roll of 15 million people.[8]

---

[4] *Oversight of the U.S. Department of Justice*, before the H. Comm. on the Judiciary, Nov. 17, 2017.

[5] Exec. Order No. 13800 (May 11, 2017), requires Cabinet members to complete reviews of their departments' effectiveness at detecting hacking by June 23, 2017.

[6] Letter from Ranking Member Jerrold Nadler, et al., to U.S. Attorney General Jeff Sessions, U.S. Dept. of Justice, Dec. 1, 2017.

[7] Geoff Mulvihill & Jake Pearson, *Federal government notifies 21 states of election hacking*, WASH. POST, Sept. 23, 2017; Cynthia McFadden et al., *Russians penetrated U.S. voter systems, says top U.S. official*, NBC, Feb. 7, 2018.

[8] Massimo Calabresi, *Inside the Secret Plan to Stop Vladimir Putin's U.S. Election Plot*, TIME, July 20, 2017.

- Foreign actors are believed to have infiltrated Florida, Colorado, New Mexico, South Carolina, and Arizona's electoral systems, as well as an election software/device provider.[9]
- Sensitive data on Georgia's 6.7 million voters, passwords used by county officials to access elections management files, and the critical e-pollbooks used to verify registered votes on Election Day were exposed by significant election infrastructure security gaps.[10] In addition, key electronic voter logs were stolen prior to the Georgia special election[11] and entire election servers had their data wiped clean.[12]
- The Russian cutout known as "Fancy Bear," which was responsible for hacking the Democratic National Committee, continues to target political organizations in various countries—including the U.S. Senate, in a recently reported operation.[13]
- Computer security experts have uncovered potential points of infiltration of the "voting infrastructure at any point in the supply chain process [allowing for] the ability to synchronize and inflict large-scale damage" particular in foreign-manufactured parts.[14]
- A study found consolidation in the voting machine and software industry—where the number of voting machine companies has dropped from nineteen to three[15]—and the resulting market structure, coupled with ineffective government action, has limited growth, stagnated innovation, and contributed to a crisis in America's election technology sector.[16]

It is our Committee's responsibility to examine the vulnerabilities and risks facing our election processes and infrastructure in order to protect the right to vote for every American—a right that includes not just equal voting rights and access to the polls, but also confidence in the accuracy and security of our election systems.

For these reasons, we urge you to hold immediate hearings on this fundamental issue.

---

[9] *Id.* (Recorded IP fingerprints pointed to Fancy Bear and Cozy Bear, cyber arms of the GRU (Russian military intelligence), as the culprits). A leaked NSA document shows that Russian hackers targeted and compromised a Florida-based voting-equipment vendor and used the stolen information to target state election officials. NATIONAL SECURITY AGENCY, RUSSIA/CYBERSECURITY: MAIN INTELLIGENCE DIRECTORATE CYBER ACTORS *** TARGET U.S. COMPANIES AND LOCAL U.S. GOVERNMENT OFFICIALS USING VOTER REGISTRATION-THEMED EMAILS, SPOOF ELECTION-RELATED PRODUCTS AND SERVICES, RESEARCH ABSENTEE BALLOT EMAIL ADDRESSES; AUGUST TO NOVEMBER 2016 (2017).

[10] Kim Zetter, *Will the Georgia Special election Get Hacked?*, POLITICO MAG., June 14, 2017.

[11] Christopher Wallace, *New Details Emerge in Theft of Georgia Voting Machines*, FOX NEWS, Apr. 18, 2017.

[12] Frank Bajak, *Georgia Election Server Wiped After Suit Filed*, AP NEWS, Oct. 27 2017.

[13] Feike Hacquebord, *Updated on Pawn Storm: New Targets and Politically Motivated Campaigns*, TREND MICRO, Jan. 12, 2018; Natasha Bertrand, *Russian hackers are laying the groundwork to spy on the US Senate, cybersecurity firm says*, BUS. INSIDER, Jan. 12, 2018.

[14] Matt Blaze et al., DEFCON25, VOTING MACHINE HACKING VILLAGE, REPORT ON CYBER VULNERABILITIES IN U.S. ELECTION EQUIPMENT, DATABASES, AND INFRASTRUCTURE (Sept. 2017).

[15] JOHN R. PATRICK, ELECTION ATTITUDE: HOW INTERNET VOTING LEADS TO A STRONGER DEMOCRACY (2016).

[16] U. PENN, WHARTON PUB. POL'Y INITIATIVE, THE BUSINESS OF VOTING: MARKET STRUCTURE AND INNOVATION IN THE ELECTION TECHNOLOGY INDUSTRY (2017).

Sincerely,