805 Fifteenth Street NW, Suite 800 Washington, DC 20005
T 202.833.1200 www.commoncause.org

COMMON CAUSE
Holding Power Accountable

June 23, 2017

The Honorable Richard Burr
Chairman
United States Senate Select Committee on Intelligence
United States Senate
Washington, DC 20510

The Honorable Mark Warner
Vice Chairman
United States Senate Select Committee on Intelligence
United States Senate
Washington, DC 20510

Dear Senators:

On behalf of Common Cause's 850,000 members and supporters committed to open and accountable government, we commend you for holding yesterday's hearing about vulnerabilities to the security of our election administration systems. We strongly encourage the Committee to vigorously pursue the investigation of the attack on those systems by the Russian government and agree to push for major improvements to cybersecurity in our elections, as discussed in this letter. This threat to our democracy cannot be overstated and your work to mitigate it is vitally important to our nation's security.

Every eligible American—Republican, Democrat, and Independent—deserves the freedom to vote and have their ballot counted as cast. Unfortunately, as yesterday's hearing demonstrated, some foreign nations are working to undermine this bedrock freedom and attack elements of state election administration systems.

Specifically, as the American intelligence community assessed earlier this year, the Russian government has "demonstrated a significant escalation in directness, level of activity, and scope of effort" to "undermine the US-led liberal democratic order."[1]

As an earlier unclassified assessment from the Office of the Director of National Intelligence indicated, Russia deployed cyber weapons to attack our election infrastructure. We know from intelligence reports that they gained access to state and local election boards,[2] and from the Department of Homeland Security that they targeted

[1] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, INTELLIGENCE COMMUNITY ASSESSMENT, ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS at ii.
[2] *Id.* at 2, 3.

21 states' election systems in 2016. [3] They have also attempted to infiltrate voting system vendors using spear phishing techniques.[4]

Our elections remain a high value target for foreign adversaries. We should expect future attacks. Congressional midterms are less than 18 months away. Gubernatorial elections in Virginia and New Jersey will take place later this year.

If a foreign military had breached state election offices in a physical way, there would be a national military response. But because the attack was digital, and election administration is primarily the province of state and local governments, many of whom work with private third party vendors, the response has not been as coordinated or as visible.

Other countries have responded to the threat of cyberattacks by altering how they conduct elections and count ballots. The Netherlands had a strong indication that the Russians would try to interfere with their elections. Instead of machine counting their ballots, they switched to hand counting.[5] The French have stopped all voting over the Internet (which was only in use for their parliamentary elections).[6] The British already count ballots by hand.[7]

In the United States, we have not taken these measures. Jurisdictions in fifteen states are using voting machines that leave no paper trail.[8] This means that elections cannot be the subject of an audit to confirm election results and no recount can occur. Few states conduct post-election audits that are robust enough to detect outcome-changing errors. Thirty-two states are still allowing marked ballots to be sent back by e-mail, which is the most insecure form of communication, or through a web-based platform that may or may not have undergone basic security testing.[9]

---

[3] Testimony of Jeanette Manfra, Acting Deputy Under Secretary for Cybersecurity and Communications at the Department of Homeland Security, and Dr. Samuel Liles, Acting Director, Cyber Division, Office of Intelligence and Analysis at the Department of Homeland Security, Before the United States Senate Select Committee on Intelligence (June 21, 2017), https://www.intelligence.senate.gov/sites/default/files/documents/os-jmanfra-062117.PDF.

[4] Pam Fessler, "Despite NSA Claim, Elections Vendor Denies System was Compromised in Hack Attempt," NPR, June 20, 2017, http://www.npr.org/2017/06/20/533637643/despite-nsa-claim-election-vendor-denies-system-was-compromised-in-hack-attempt.

[5] Sewell Chan, "Fearful of Hacking, Dutch Will Count Ballots by Hand," N.Y. TIMES, Feb. 1, 2017, https://www.nytimes.com/2017/02/01/world/europe/netherlands-hacking-concerns-hand-count-ballots.html.

[6] Marine Le Pennetier, "France Drops Electronic Voting for Citizens Abroad Over Cybersecurity Fears," REUTERS, Mar. 6, 2017, http://www.reuters.com/article/us-france-election-cyber-idUSKBN16D233

[7] Imogen Groome, "How Are General Election Votes Counted? All About the Results Process," METRO, June 8, 2017, http://metro.co.uk/2017/06/08/how-are-general-election-votes-counted-all-about-the-results-process-6693827/.

[8] Mike Orcutt, "A Close Election Could Expose Risky Electronic Voting Machines," M.I.T. TECHNOLOGY REVIEW, Sept. 30, 2016, https://www.technologyreview.com/s/602482/a-close-election-could-expose-risky-electronic-voting-machines/.

[9] National Conference of State Legislatures, "Electronic Transmission of Ballots," http://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx#Returning Ballots (last visited June 22, 2017).

In short, there are still several vulnerabilities that a foreign adversary could exploit to attack our voting systems—and few alarm bells would ring if they did.

As part of the Committee's investigation, Common Cause urges the Committee to establish recommendations for mandates that will better secure our election infrastructure. Americans need a coordinated, rigorous national, state, and local response to ensure that our election administration systems are resilient enough to withstand the cyberattacks of a foreign adversary moving forward. This may include designing, elevating and mandating some basic cybersecurity measures.

For example, states should replace paperless electronic voting machines with new systems that provide a voter-verified paper ballot. No one should cast their ballot over the Internet, including by web, email or fax. Election administrators should conduct risk-limiting post-election audits to ensure that election outcomes are accurate before the final results are certified. Finally, Congress should task a federal agency with taking responsibility to ensure robust, comprehensive election cybersecurity.

The security of our election systems should not divide Republican from Democrat. It must be your priority to put country over party and work together to safeguard a democracy that works for everyone.

Thank you for yesterday's important hearing, and for your work moving forward.

Sincerely,

Karen Hobert Flynn
President
Common Cause

CC:

The Honorable Roy Blunt
The Honorable Susan Collins
The Honorable John Cornyn
The Honorable Tom Cotton
The Honorable Dianne Feinstein
The Honorable Kamala Harris
The Honorable Martin Heinrich
The Honorable Angus King
The Honorable James Lankford
The Honorable Joe Manchin
The Honorable James Risch
The Honorable Marco Rubio
The Honorable Ron Wyden