

Congress of the United States
Washington, DC 20515

December 19, 2017

The Honorable Paul Ryan
Speaker of the House
H-232, United States Capitol
Washington, D.C. 20515

Dear Mr. Speaker:

We represent 18 of the 21 states whose elections were targeted by Russian hackers in 2016, and we write because we are deeply concerned about the security of America's election infrastructure. Fair, free, and secure elections are the cornerstone of our democracy. Accordingly, we respectfully request that you ask DHS and the FBI to brief all Members of Congress on the Russian attack on 21 states' voting systems, direct the relevant Congressional committees to investigate this attack, and seek bipartisan solutions to secure our elections going forward.

The attacks in 2016 were not a one-off occurrence. In March 2017, then-FBI Director James Comey testified before the House Permanent Select Committee on Intelligence that: "[T]hey'll be back. They'll be back in 2020. They may be back in 2018."¹ Days before the 2017 elections, Bob Kolasky, the acting Deputy Undersecretary of the National Protection and Programs Directorate at the Department of Homeland Security said, "We saw in 2016 that Russia had an intent to be involved in our elections and some capability to be active or to attempt to be active in scanning election systems. We have not seen any evidence that intent or capability has changed."² The threat remains, and Congress must act.

Over the past six months, the Election Security Task Force, comprised of Democratic Members of the Committee on Homeland Security and the Committee on House Administration, has conducted an in-depth examination of America's voting systems. The Task Force's preliminary findings demonstrate that this issue needs urgent, bipartisan attention.

Our voting machines can easily be hacked. In July, at DefCon, one of the world's largest, longest-running, and best-known hacker conferences, 25 pieces of election equipment were successfully breached by participants with little prior knowledge and limited tools.³ In over 40 states, elections are carried out using voting machines that were purchased more than a decade

¹ United States Cong. House. House Permanent Select Committee on Intelligence. *Open Hearing on Russian Active Measures Investigation*, March 20, 2017. 115th Congress. 1st session, 2017.

² Morgan Chalfant, "Homeland Security Cyber Unit on Alert for Election Day," *The Hill* (Nov. 4, 2017), available at <http://thehill.com/policy/cybersecurity/358710-homeland-security-cyber-unit-on-alert-for-election-day>.

³ Matt Blaze et al., *DEFCON 25 Voting Machine Hacking Village: Rep. on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, 4 (2017) <https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf>.

ago.⁴ These machines are now either obsolete or at the end of their useful life. Some of these machines rely on operating systems like Windows XP or Windows 2000 which pose a particularly significant security risk as those operating systems either do not receive regular security patches, or have stopped receiving support altogether.⁵ These issues are exacerbated by the fact that twenty percent of Americans cast their ballot on voting machines that do not have any kind of paper backup.⁶ In other words, if these paperless machines were hacked, it would be nearly impossible to tell.⁷

State voter registration databases are also vulnerable to attack. In Illinois, hackers successfully breached registration databases and attempted, but failed, to alter and delete voting records.⁸ In Arizona, hackers successfully installed malware on a county election official's computer.⁹ Russian hackers also targeted at least one election vendor with the hope of ultimately obtaining access into numerous state and local voter registration databases.¹⁰ If these attacks had been successful, hackers would have been able to alter or delete voter registration records, causing a great deal of chaos on Election Day and potentially swaying the results of the election.

State and local election officials are acutely aware of these issues, but many are struggling to get the necessary funding from their legislatures,¹¹ and are frustrated by Congressional inaction.¹² The plea for Congress to act is echoed by a bipartisan group of former government officials, academics and cyber security experts. Michael Chertoff, former Secretary of Homeland Security wrote in *The Wall Street Journal*, “[L]awmakers and election officials’ lackadaisical response is both staggering and distressing... This is a matter of national security, and Congress should treat it as such... [T]here’s a clear need for action to upgrade security systems and create meaningful standards.” In June, a group of over 100 computer scientists and cyber experts wrote to Congress to take “simple, straightforward, and cost-effective actions to set meaningful standards to protect American elections.”¹³

⁴ Lawrence Norden & Ian Vanderwalker, Brennan Center for Justice at NYU School of Law, *Securing Elections from Foreign Interference*, 9 (2017).

⁵ *Id.*

⁶ Norden & Vandewalker, 11.

⁷ Eric Geller, *Virginia Bars Voting Machines Considered Top Hacking Target*, POLITICO (Sept. 8, 2017) <http://www.politico.com/story/2017/09/08/virginia-election-machines-hacking-target-242492>.

⁸ Pam Fessler, *10 Months After Election Day, Feds Tell States More About Russian Hacking*, NPR (Sept. 22, 2017) <https://www.npr.org/2017/09/22/552956517/ten-months-after-election-day-feds-tell-states-more-about-russian-hacking>.

⁹ *Id.*

¹⁰ Matthew Cole et al., *Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election*, *The Intercept* (June 5, 2017) <https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/>.

¹¹ Cory Bennett et al., *Cash-Strapped States Brace for Russian Hacking Fight*, POLITICO (Sept. 3, 2017), <http://www.politico.com/story/2017/09/03/election-hackers-russia-cyberattack-voting-242266>.

¹² Reid Wilson, *Election Officials Race to Combat Cyberattacks*, *The Hill* (Nov. 8, 2017) <http://thehill.com/homenews/campaign/359243-election-officials-race-to-combat-cyberattacks>.

¹³ National Election Defense Coalition, *Expert Sign-On Letter to Congress: Secure American Elections* (2017). <https://www.electiondefense.org/election-integrity-expert-letter/>.

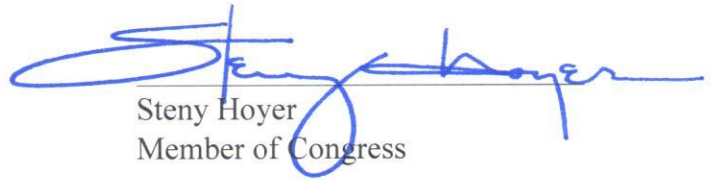
When a sovereign nation attempts to meddle in our elections, it is an attack on our country. We urge you to recognize that ensuring the security and integrity of our election system is a bipartisan issue, to request a briefing for all Members of Congress from DHS and the FBI, and to direct the relevant committees to open an investigation on securing America's election infrastructure.

Thank you for your attention to this matter.

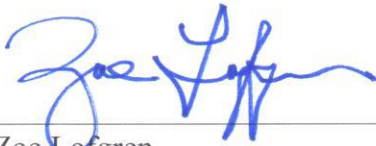
Sincerely,



Robert A. Brady
Member of Congress



Steny Hoyer
Member of Congress



Zoe Lofgren
Member of Congress



Val Butler Demings
Member of Congress



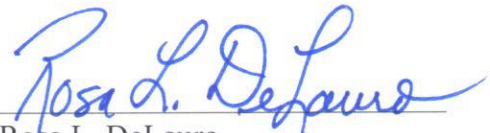
Lisa Blunt Rochester
Member of Congress



Peter DeFazio
Member of Congress



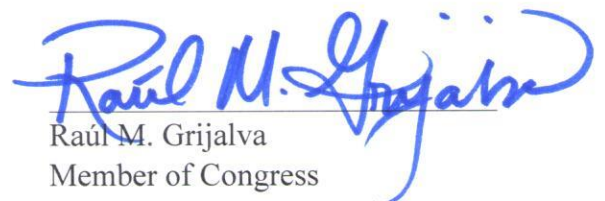
Diana DeGette
Member of Congress



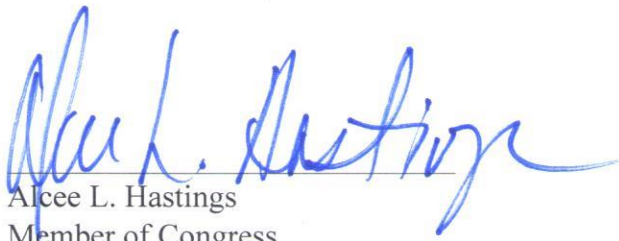
Rosa L. DeLauro
Member of Congress



Gene Green
Member of Congress



Raúl M. Grijalva
Member of Congress



Alice L. Hastings
Member of Congress



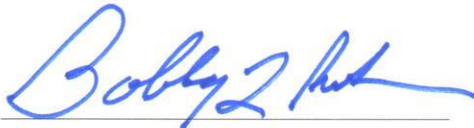
Marcy Kaptur
Member of Congress



Ron Kind
Member of Congress



Dave Loebsack
Member of Congress



Bobby L. Rush
Member of Congress



John Sarbanes
Member of Congress



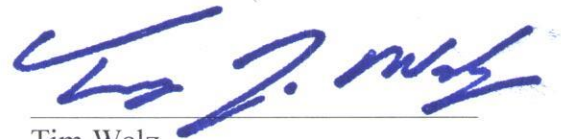
Robert C. "Bobby" Scott
Member of Congress



Terri Sewell
Member of Congress



Adam Smith
Member of Congress



Tim Walz
Member of Congress



Maxine Waters
Member of Congress