

**Congress of the United States**  
**Washington, DC 20515**

November 16, 2017

The Honorable Rodney P. Frelinghuysen  
Chairman  
Committee on Appropriations  
U.S. House of Representatives  
Washington, D.C. 20515

The Honorable Nita M. Lowey  
Ranking Member  
Committee on Appropriations  
U.S. House of Representatives  
Washington, D.C. 20515

Dear Chairman Frelinghuysen and Ranking Member Lowey:

As you and your colleagues prepare to finalize appropriations legislation for FY 2018, we respectfully request that you appropriate the remaining \$400 million from the Help America Vote Act of 2002 (HAVA) for states to use to secure their elections infrastructure.<sup>1</sup> We know now that Russia launched an unprecedented assault on our elections in 2016, targeting 21 states' voting systems, and we believe this money is necessary to protect our elections from future attack.

Over the past five months, we have co-chaired an Election Security Task Force to better understand what can be done to protect our elections going forward. Our findings demonstrate that there is an urgent need for federal funding to help states secure their elections.

Through our investigation, we found that 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.<sup>2</sup> In over 40 states, elections are carried out using voting machines that were purchased more than a decade ago.<sup>3</sup> 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.<sup>4</sup> 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.<sup>5</sup> In other words, if these paperless machines were hacked, it would be nearly impossible to tell.<sup>6</sup>

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.<sup>7</sup> In

---

<sup>1</sup> Pub. L. 107-252 (Oct. 29, 2002).

<sup>2</sup> 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>.

<sup>3</sup> Lawrence Norden & Ian Vanderwalker, Brennan Center for Justice at NYU School of Law, *Securing Elections from Foreign Interference*, 9 (2017).

<sup>4</sup> *Id.*

<sup>5</sup> Norden & Vandewalker, 11.

<sup>6</sup> 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>.

<sup>7</sup> Pam Fessler, *10 Months After Election Day, Feds Tell States More About Russian Hacking*, NPR (Sept. 22, 2017).



Arizona, hackers successfully installed malware on a county election official's computer.<sup>8</sup> Russian hackers also targeted at least one election vendor with the hope of ultimately obtaining access into numerous state and local voter registration databases.<sup>9</sup> 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.

The single most urgent need is for states using paperless machines to replace their outdated equipment with paper ballot voting systems. The Brennan Center estimates that cost to replace paperless voting machines would be between \$130 and \$400 million, and states do not have the money to do this themselves.<sup>10</sup> South Carolina is one of the five remaining states that relies exclusively on paperless machines, and a spokesman for the South Carolina Election Commission recently told the New York Times, "We're using the same equipment we've used since 2004. If \$40 million dropped into our hands today, we'd have a paper ballot trail, too."<sup>11</sup> In order to prevent future attacks, states also need to hire IT staff, upgrade and maintain IT infrastructure, and train election officials and poll workers on cybersecurity.

State and local election officials are acutely aware that they need to improve election security, but they lack the necessary funds to safeguard their voting infrastructure.<sup>12</sup> In most states, legislatures are not increasing their election security budgets.<sup>13</sup> In some cases, Governors are actively undermining election security efforts. In Florida, Governor Scott's budget proposed reducing the funding for the Division of Elections by almost one million dollars.<sup>14</sup> In July, Governor Kasich vetoed a provision in Ohio's budget that would have allocated one million dollars towards voting equipment.<sup>15</sup> Governor Walker issued a partial veto to the state's budget, and in doing so, eliminated five jobs from the Wisconsin Elections Commission.<sup>16</sup> This issue is simply too important to sit back and watch state governments and the federal government pass responsibility back and forth.

Moreover, state and local officials have expressed a desire for Congress to step in. In a recent *Politico* survey of state election officials, 21 of 33 respondents want the federal government to authorize funds

---

<https://www.npr.org/2017/09/22/552956517/ten-months-after-election-day-feds-tell-states-more-about-russian-hacking>

<sup>8</sup> *Id.*

<sup>9</sup> 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/>.

<sup>10</sup> Norden & Vandewalker, 11

<sup>11</sup> Michael Wines, *Wary of Hackers, States Move to Upgrade Voting Systems*, The New York Times (October 14, 2017) [https://www.nytimes.com/2017/10/14/us/voting-russians-hacking-states-.html?\\_r=0](https://www.nytimes.com/2017/10/14/us/voting-russians-hacking-states-.html?_r=0).

<sup>12</sup> 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>

<sup>13</sup> 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>

<sup>14</sup> Governor Rick Scott's 2017-2018 Budget, (last visited, Oct. 18, 2017) <http://fightingforfloridasfuturebudget.com/web%20forms/Budget/BudgetService.aspx?rid1=327714&rid2=298915&ai=45000000&title=STATE>.

<sup>15</sup> Jackie Borchardt, *Ohio Gov. John Kasich Vetoes Medicaid Freeze, Signs State Budget Bill*, Cleveland.com (July 10, 2017) [http://www.cleveland.com/metro/index.ssf/2017/06/ohio\\_gov\\_john\\_kasich\\_signs\\_sta.html](http://www.cleveland.com/metro/index.ssf/2017/06/ohio_gov_john_kasich_signs_sta.html).

<sup>16</sup> Veto Message in Brief, Sept. 20, 2017, p. 13. <https://walker.wi.gov/sites/default/files/09.20.17%20Veto%20Message%20in%20Brief.pdf>.



for states to spend on replacing voting machines or otherwise strengthening election security.<sup>17</sup> In response to the letter sent out by the Task Force to the chief election official in each state asking how the federal government could help states with election security, the National Association of Secretaries of States replied by saying, “States would clearly benefit from the appropriation of the outstanding balance of federal HAVA funds to aid them in ensuring that they have sufficient equipment, technical support, and resources to maintain a sound security posture for their computer-based systems.”<sup>18</sup>

The money that states need can be appropriated right now. HAVA authorized \$3 billion dollars for states to upgrade and modernize their election infrastructure in the wake of the chaotic 2000 presidential election. According to the Election Assistance Commission, the agency charged with administering HAVA’s grants, approximately \$2.6 billion of the HAVA funds have been distributed.<sup>19</sup> Appropriating the remaining \$400 million would enable states to take the crucial security steps of replacing outdated equipment, implementing cybersecurity best practices, and hiring IT staff.

When a sovereign nation attempts to meddle in our elections, it is an attack on our country. We cannot leave states to defend against the sophisticated cyber tactics of state actors like Russia on their own. Michael Chertoff, former Secretary of Homeland Security wrote in The Wall Street Journal, “In an age of unprecedented cyber risks, these dangers aren’t surprising. But lawmakers and election officials’ lackadaisical response is both staggering and distressing...This is a matter of national security, and Congress should treat it as such.” We urge you to recognize that ensuring the security and integrity of our election system is a bipartisan issue, and to appropriate the funds states desperately need to secure their elections.

Thank you for your attention to this matter.

Sincerely,



ROBERT A. BRADY  
Ranking Member  
Committee on House Administration  
U.S. House of Representatives



BENNIE G. THOMPSON  
Ranking Member  
Committee on Homeland Security  
U.S. House of Representatives

---

<sup>17</sup> Bennett.

<sup>18</sup> Letter from Connie Lawson, President, National Association of Secretaries of State, to Congressman Bennie Thompson & Congressman Robert Brady, Co-Chairman, Joint Task Force on Election Security (Aug. 3, 2017) (on file with author).

<sup>19</sup> U.S. Election Assistance Commission, *Annual Grant Expenditure Report Fiscal Year 2015*, 6 <https://www.eac.gov/documents/2016/4/11/final-fy-2015-grants-reportpdf/>.