Center for American Progress

On HAVA's 15th Anniversary, Congress Needs to Make U.S. Elections More Secure

By Michael Sozan October 26, 2017

On October 29, 2002, then-President George W. Bush signed the Help America Vote Act (HAVA) into law.[1] The historic deadlocked presidential election of 2000 had just spurred the U.S. Congress to pass sweeping reforms to America's election infrastructure. With bipartisan cooperation, Congress passed HAVA[2] in order to prevent a repeat of the electoral crisis that ensued during the 2000 election.

Last year, when Russian agents tried to hack into U.S. election systems during the 2016 presidential election cycle, U.S. election infrastructure once again experienced a crisis that exposed continuing vulnerabilities.[3] In light of the serious national security threats implicated by these unprecedented cyberattacks, it is time for Congress to act in the spirit of HAVA, 15 years after it was originally passed, and take immediate steps to shore up U.S. election infrastructure and invest in the security of America's elections.

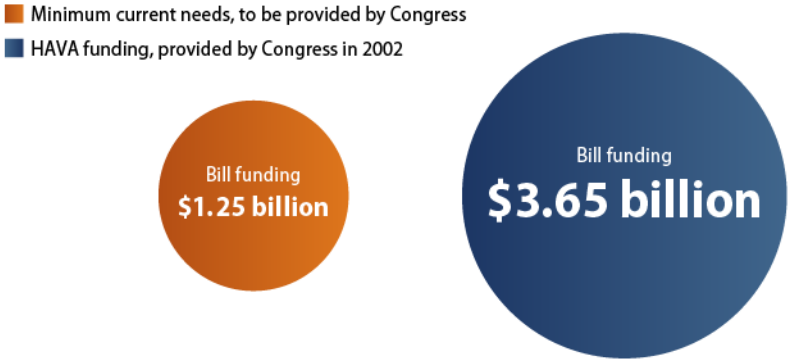
The post-2000 reforms embodied in HAVA revealed Congress' intent to act boldly to protect one of the United States' most bedrock constitutional rights: the right of every eligible American to cast a ballot that is properly counted. Through HAVA, Congress set forth requirements for voting equipment. Critically, HAVA authorized much-needed federal funding—$3.65 billion—to the states in order to meet the new statutory requirements.[4] Due to this infusion of federal funds, voting machines became more reliable, though still not impervious to hacking or malfeasance. Today, many post-HAVA voting machines are more than 10 years old and nearing the end of their expected life cycles.[5] These aging machines can have major flaws that render them insecure and vulnerable, which is unacceptable given U.S. adversaries' attempts to hack into state and local election infrastructure.[6]

Now, in 2017, Congress can provide the next phase of necessary resources to help defend state and local elections systems from future cyberattacks for a fraction of HAVA's $3.65 billion in funding. A sum of $1.25 billion over a 10-year period would provide the minimum necessary funds to cover a one-time cost of $1 billion to update outdated voting machines; $5 million per year to conduct threat assessments for voter registration databases; and $20 million per year to conduct nationwide risk-limiting audits for federal elections.[7]

FIGURE 1

Safeguarding America's votes

Help America Vote Act funding vs. current necessary funding, in billions of dollars



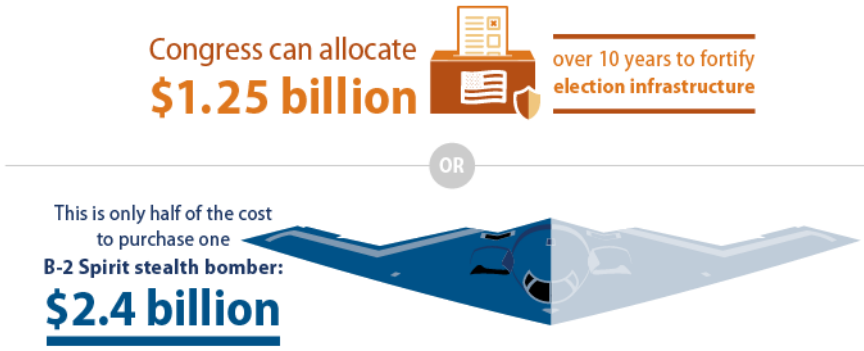
Sources: Arthur L. Burris and Eric A. Fischer, "The Help America Vote Act and Election Administration: Overview and Selected Issues for the 2016 Election" (Washington: Congressional Research Service, 2016), available at https://fas.org/sgp/crs/misc/RS20898.pdf.; Lawrence Norden and Christopher Famighetti, "America's Voting Machines at Risk" (New York: Brennan Center for Justice, 2015), pp. 17, 19, available at https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf; transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 2," June 21, 2017. Provided to author by Bloomberg Government, July 30, 2017. On file with author.

These measures are vital for bolstering the United States' national security, and funding them should be considered as necessary to protecting America's democracy as military spending. For the cost of half of one B-2 Spirit bomber or four F-22 Raptor aircrafts—both of which are also used to protect the nation from foreign threats—Congress could take steps to secure the U.S. election infrastructure from foreign enemies.[8] Surely protecting America's election infrastructure from attack is as crucial to protecting U.S. democracy as paying for one-half of a military aircraft.

FIGURE 2

National security priorities

Costs to fortify election infrastructure vs. costs of expensive military equipment



Source: *TIME*, "Top 10 Most Expensive Military Planes," available at http://content.time.com/time/photogallery/0,29307,1912203_1913325,00.html (last accessed October 2017).

Federal lawmakers of both parties want to increase election security

Fortunately, there is bipartisan legislation in the U.S. Senate and U.S. House of Representatives that would take major steps toward protecting the United States' election infrastructure: a commonsense provision introduced by Sens. Amy Klobuchar (D-MN) and Lindsey Graham (R-SC) as an amendment to the National Defense Authorization Act of 2017 (NDAA)[9]—and its House counterpart, the Protecting the American Process for Election Results (PAPER) Act, introduced by Reps. Jim Langevin (D-RI) and Mark Meadows (R-NC).[10] This bipartisan legislation would allow states to request a Department of Homeland Security (DHS) security risk and vulnerability assessment and, after undergoing the assessment, would receive grant funding to implement security recommendations. Additionally, this legislation would require the U.S. Election Assistance Commission—an agency created by HAVA—to hold public hearings; work with experts to establish best practices for both election cybersecurity and election audits; and provide funding for states to implement those best practices. Moreover, the bill would task the DHS and the director of national intelligence with establishing strong lines of communication with state election officials regarding cyberthreats and would allow each state's senior election official to receive a security clearance to receive briefings on cyberthreats. Finally, the legislation would require states to take steps toward ensuring that voter-verified paper ballot auditing systems are in place.

The Klobuchar-Graham legislation has not yet received a vote in the Senate, but it did garner the support of the U.S. Senate Committee on Armed Services Chairman John McCain (R-AZ)[11] and Senate Minority Leader Chuck Schumer (D-NY) during debate on the NDAA.[12] On the House side, the PAPER Act has not yet received consideration.[13]

Multiple national security leaders—of both political parties—have voiced support for this bipartisan legislation, including former Secretary of Homeland Security Michael Chertoff, former CIA Director James Woolsey, and former House Permanent Select Committee on Intelligence Chairman Mike Rogers, who wrote to Senate leaders and the Senate Committee on Armed Services leadership on September 11, 2017, to support the effort. The leaders stated, in part, "Although election administration is the province of state and local governments, the federal government has a responsibility to support the states and 'provide for the common defense.' … We do not expect the states to defend themselves against kinetic attacks by hostile foreign powers, nor should we leave them to defend against foreign cyberattacks on their own."[14] In the wake of this broad support from national security leaders and lawmakers of both parties, Congress should pass this legislation—coupled with an adequate funding authorization of at least $1.25 billion—immediately.

Notably, other election security legislation could soon be introduced, as additional federal lawmakers of both major political parties are stepping up to show leadership on the issue. For example, Sens. Kamala Harris (D-CA) and James Lankford (R-OK),

both members of the Senate Permanent Select Committee on Intelligence and Senate Committee on Homeland Security and Government Affairs, continue to work on policies to improve election infrastructure.[15]

It is imperative that Congress act now

The United States has nonpresidential federal elections coming up in 2018 and the presidential election in 2020. The foundation of the United States' democratic self-government relies on free and fair elections; thus, when the security of those elections is undermined, Americans may begin to question the value of their vote. This, in turn, damages U.S. democracy. Alarmingly, a July 2017 poll found that 1 in 4 Americans will consider not participating in future elections due to concerns over cybersecurity and the worry that their vote will not be protected.[16]

No one yet knows the full extent of Russian attempts to hack into state and local election systems in 2016. But credible evidence shows that Russians tried to hack at least 20 state election systems before Election Day and sent messages to 122 email addresses associated with entities likely involved in the management of voter registration systems in order to probe or infiltrate voting databases.[17] Hackers did, in fact, breach election records in Illinois, where they tried to delete and alter voter information.[18]

Even worse, the 2016 election cycle may only be the tip of the iceberg of what may happen in future elections, according to intelligence experts and federal lawmakers.[19] Russia may have used the 2016 cycle to find vulnerabilities in U.S. election databases to prepare for more aggressive intrusions in the midterm congressional elections of 2018 and the next presidential election in 2020.[20] Other hostile actors, such as Iran, North Korea, and the Islamic State group, have also used cyberattacks or the internet to try to subvert Western democracies—and they may try again.[21]

Unfortunately, as evinced in a recent hacking simulation, U.S. election infrastructure—maintained principally by states and localities in more than 7,000 election jurisdictions nationwide—is not prepared to defend against future interference.[22] These voting systems include inadequate cybersecurity measures for voting machines and databases; outdated voting machines; and a lack of verified paper ballots or records, which are imperative to conducting appropriate audits. To compound matters, most states and localities simply lack the necessary funds to address these problems.[23]

State and local officials increasingly recognize that protecting U.S. elections is not just a matter of ensuring fair elections but also one of national security that requires coordination at all levels of government—federal, state, and local. Before Election Day in November 2016, 33 states and 36 localities requested that the DHS assess their election systems.[24] More requests have been made in 2017.[25] DHS officials are attaching

greater urgency to this issue. In January 2017, then-Secretary of Homeland Security Jeh Johnson designated state and local election systems as "critical infrastructure"[26]—like the banking sector and the electrical grid—and the DHS has established a coordinating council to work directly with states on bolstering election security.[27] But under current law, these important steps do not provide local jurisdictions with the broad range of resources and funds to modernize their election infrastructure.

Conclusion

In light of these circumstances, Congress must seize the initiative now to fortify the security of U.S. election infrastructure. This is a rare chance for Congress to act in a bipartisan and timely manner. And as the 15th anniversary of HAVA infusing billions of dollars to upgrade voting machines approaches, there should be increased urgency for federal lawmakers to set aside partisan differences and pass much-needed election infrastructure legislation. Election security is a matter of national security, and these affairs historically have been above the political fray. Russian attempts to hack into the U.S. 2016 election, regardless of whom they favored or whether they were successful, dictate that Congress take decisive action to shore up the public's confidence in the security of U.S. elections and help protect this country's democracy.

Michael Sozan is a senior fellow supporting the work of the Democracy and Government Reform team at the Center for American Progress.

Endnotes

1 In December 2001, the U.S. House of Representative passed HAVA—H.R. 3295. The Senate passed similar legislation in early 2002—S. Res 565. The two chambers resolved the differences in the legislation via a conference committee, and the final version of HAVA passed each chamber in October 2002 before being signed into law by then-President George W. Bush. For a helpful history of HAVA, see Arthur L. Burris and Eric A. Fischer, "The Help America Vote Act and Election Administration: Overview and Selected Issues for the 2016 Election" (Washington: Congressional Research Service, 2016), available at https://fas.org/sgp/crs/misc/RS20898.pdf.

2 *Help America Vote Act of 2002*, Public Law 252, 107th Cong., 2d sess. (October 29, 2002), available at https://www.gpo.gov/fdsys/pkg/PLAW-107publ252/pdf/PLAW-107publ252.pdf.

3 Office of the Director of National Intelligence, *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution* (National Intelligence Council, 2017), available at https://www.dni.gov/files/documents/ICA_2017_01.pdf.

4 Burris and Fischer, "The Help America Vote Act and Election Administration," Table 2.

5 Lawrence Norden and Christopher Famighetti, "America's Voting Machines at Risk," p. 4 (New York: Brennan Center for Justice, 2015), available at https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf

6 Norden and Famighetti, "America's Voting Machines at Risk," p. 5.

7 Ten years is the standard time period used for federal budget scoring. These dollar figures are derived from the following sources: Norden and Famighetti, "America's Voting Machines at Risk," pp. 17 and 19; transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 2," June 21, 2017. Provided to author by Bloomberg Government, July 30, 2017. On file with author.

8 *Time*, "Top 10 Most Expensive Military Planes," available at http://content.time.com/time/photogallery/0,29307,1912203_1913325,00.html (last accessed October 2017); AviationCV.com, "Top 5 Most Expensive Military Aircraft," available at https://www.aviationcv.com/aviation-blog/2016/top-5-most-expensive-military-aircraft\ (last accessed October 2017).

9 Congress.gov, "S.Amdt.656 to H.R.2810," available at https://www.congress.gov/amendment/115th-congress/senate-amendment/656 (last accessed October 2017); Niels Lesniewski, "Bipartisan Push for Electoral Security Gets Priority Status," *Roll Call*, September 12, 2017, available at www.rollcall.com/news/politics/klobuchar-graham-lead-push-counter-russia-better-election-security.

10 *Protecting the American Process for Election Results Act*, H.R. 3751, 115 Cong., 1 sess. (_____2017).

11 See Kyle Cheney, Elana Schor, and Cory Bennett, "Senate Democrats worry Russia could jeopardize reelection bids," *Politico*, October 11, 2017, available at http://www.politico.com/story/2017/10/11/senate-democrats-worry-russia-could-jeopardize-reelection-bids-243645.

12 See Senate Democrats, "Schumer Floor Remarks on NDAA and President Trump's Election Integrity Commission," Press release, September 12, 2017, available at https://www.democrats.senate.gov/newsroom/press-releases/schumer-floor-remarks-on-ndaa-and-president-trumps-election-integrity-commission.

13 *Protecting the American Process for Election Results Act*.

14 Lesniewski, "Bipartisan Push for Electoral Security Gets Priority Status."

15 See Office of Sen. Kamala D. Harris, "Senator Harris Questions DHS and FBI Reps on Insufficient Notifications Between State, Local, and Federal Officials on Election Breaches," Press release, June 21, 2017, available at https://www.harris.senate.gov/content/senator-harris-questions-dhs-and-fbi-reps-insufficient-notifications-between-state-local-and; Cheney, Schor, and Bennett, "Senate Democrats worry Russia could jeopardize reelection bids." Sen. James Lankford (R-OK) remarked in this article, "[W]e … want to be able to help states trying to defend themselves against a foreign adversary."

16 See Megan Trimble, "Hacking Fears May Stop 1 in 4 Voters From Casting Ballots," U.S. News and World Report, July 12, 2017, available at https://www.usnews.com/news/national-news/articles/2017-07-12/1-in-4-voters-may-not-vote-in-2018-midterms-because-of-cybersecurity-concerns. As Sen. Marco Rubio (R-FL) noted in the following transcript, "[I]t is really critical that people have confidence that when they go vote that vote is going to count and someone's not going to come in electronically and change it." See transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 1," June 21, 2017. Provided to authors by Bloomberg Government, July 30, 2017.

17 Patrick Marley and Jason Stein, "Russians Tried to Hack Election Systems of 21 States in 2016, Officials Say," *USA Today*, September 22, 2017, available at https://www.usatoday.com/story/news/nation-now/2017/09/22/wisconsin-one-20-states-targeted-russian-hacking-elections-systems-2016/694719001/; Michael Riley and Jordan Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known," Bloomberg, June 13, 2017, available at https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections; Matthew Cole and others, "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election," The Intercept, June 5, 2017, available at https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.

18 Riley and Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known."

19 See, for example, Ryan Teague Beckwith, "Read the Transcript of James Comey's Testimony," *Time*, June 8, 2017, available at http://time.com/4810345/james-comey-testimony-real-time-transcript/.

20 Nicholas Fandos, "Senate Intelligence Heads Warn That Russian Election Meddling Continues," *The New York Times*, October 4, 2017, available at https://www.nytimes.com/2017/10/04/us/politics/senate-intelligence-committee-russia-election-trump.html.

21 Gordon Corera, "NHS cyber-attack was 'launched from North Korea,'" BBC, June 16, 2017, available at http://www.bbc.com/news/technology-40297493; Kim Sengupta, "Isis-linked hackers attack NHS websites to show gruesome Syrian civil war images," The *Independent*, February 7, 2017, available at http://www.independent.co.uk/news/uk/crime/isis-islamist-hackers-nhs-websites-cyber-attack-syrian-civil-war-images-islamic-state-a7567236.html; Dustin Volz and Jim Finkle, "U.S. indicts Iranians for hacking dozens of banks, New York dam," Reuters, March 24, 2016, available at http://www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WQ1JF; Josh Gerstein, "2 Iranians charged in hacking case where Obama pardoned another," *Politico*, July 17, 2017, available at http://www.politico.com/blogs/under-the-radar/2017/07/17/iranians-charged-in-hacking-case-obama-pardoned-240643.

22 See Greg Gordon, "Cyber experts were blocked in their push to patch voting systems in 2016," McClatchy, August 29, 2017, available at http://www.mcclatchydc.com/news/nation-world/national/article170006067.html; Matt Blaze and others, "Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure" (Las Vegas: DEFCON 25 Voting Machine Hacking Village, 2017), available at https://www.defcon.org/images/defcon-25/DEFCON25votingvillagereport.pdf.

23 Cory Bennett and others, "Cash-strapped states brace for Russian hacking fight," *Politico*, September 3, 2017, available at http://www.politico.com/story/2017/09/03/election-hackers-russia-cyberattack-voting-242266; Michael Wines, "Wary of Hackers, States Move to Upgrade Voting Systems," *The New York Times*, October 14, 2017, available at https://www.nytimes.com/2017/10/14/us/voting-russians-hacking-states-.html.

24 Jeremy Herb, "First on CNN: 33 states, 36 localities asked DHS for help protecting election systems," CNN, August 2, 2017, available at http://www.cnn.com/2017/08/02/politics/cyber-hacking-russia-states/index.html.

25 Ibid.

26 U.S. Department of Homeland Security, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," Press release, January 6, 2017, available at https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

27 See Cheney, Schor, and Bennett, "Senate Democrats worry Russia could jeopardize reelection bids"; Wines, "Wary of Hackers, States Move to Upgrade Voting Systems."