Center for American Progress

9 Solutions to Secure America's Elections

By Danielle Root and Liz Kennedy August 16, 2017

The legitimacy of self-government rests on the consent of the governed. In our democratic republic, that consent is manifested through the administration of free and fair elections. But in 2016, our democratic process came under attack from a foreign state seeking to exercise power and influence in U.S. domestic politics. It's possible that Russia believed that if it could interfere in the U.S. presidential election, it could change the course of American history.

Last summer, Americans learned that Russian operatives were behind leaks at the Democratic National Committee (DNC).[1] Those leaks exposed sensitive information about DNC staffers, including Social Security numbers, home addresses, and personal details that resulted in harassment, attempts at identity theft, and workplace marginalization.[2] In January 2017, the country's intelligence community unanimously confirmed that the Russian government—under orders from Russian President Vladimir Putin—interfered in the 2016 elections, engaging in a mass disinformation campaign to assist Donald Trump in winning the presidential election.[3]

That was only the beginning. In June 2017, reports surfaced that Russian hackers infiltrated 39 state election systems in the lead-up to Election Day, while a top secret National Security Agency (NSA) report published by The Intercept in July revealed that Russian military intelligence, or the Main Intelligence Directorate (GRU), sent spear-phishing emails to 122 email addresses associated with those likely "involved in the management of voter registration systems" in an attempt to probe or infiltrate voting databases.[4] After successfully breaching election records in Illinois, hackers attempted to delete and alter voter information. The Illinois database contained the personal information—including names, birthdates, gender, driver's license numbers, and partial Social Security numbers—of 15 million people.[5] Bloomberg estimates that as many as 90,000 records were compromised.[6]

According to the U.S. Department of Homeland Security (DHS), there are no signs, as yet, that Russia tampered with vote totals or succeeded in removing eligible Americans from state voting lists.[7] But we still do not have a full picture of what the Russians were doing, and the FBI has said that it is conducting multiple investigations into what happened.[8]

Intelligence experts warn that the 2016 U.S. election cycle is only a preview of what's to come.[9] Russia may have used the 2016 cycle as a testing ground to determine vulnerabilities in U.S. election databases in preparation for more sophisticated campaigns in future elections. As Sen. Angus King (I-ME) warned, "[T]hey are going to be back, and they're going to be back with knowledge and information that they didn't have before."[10]

Russia is not the only U.S. adversary honing its skills in cyberintrusion. North Korea and Iran have also engaged in destructive cyberattacks against Western democracies, and the Islamic State has made strategic use of the internet to advance its goals.[11]

Unfortunately, our election infrastructure is woefully ill-prepared for future interference. Outdated voting machines, lack of verified paper ballots or records, and inadequate cybersecurity measures for voting machines and databases are just a few vulnerabilities that leave U.S. elections open to subversion by hostile entities—foreign and domestic—seeking to undermine the democratic process and even skew election results.[12] While further efforts are needed to address the wider influence campaign that extended well beyond election systems, it is of extreme importance that America begins to invest in and update its election infrastructure to protect against future interference and disruption.[13]

Protecting our elections is a matter of national security, requiring immediate action and coordination at all levels of government. In the lead-up to the 2016 general election, 33 states, along with 36 localities, requested assessment of their election systems by DHS.[14] More requests have been made since November 2016.[15] For its part, DHS has made clear, "[T]his is of the utmost urgency for the department and this government to ensure that we have better protections going forward."[16] Election officials and politicians at the local, state, and federal levels have a critical role to play.

This issue brief details nine recommendations to address some of the most serious vulnerabilities in America's election infrastructure:

1. Require voter-verified paper ballots or records for every vote cast.

2. Replace old voting machines.

3. Conduct robust postelection audits to confirm election outcomes.

4. Update and secure outdated voter registration systems and e-poll books.

5. Require minimum cybersecurity standards for voter registration systems and other pieces of voting infrastructure.

6. Perform mandatory pre-election testing on all voting machines, as well as continuous vulnerability analysis.

7. Expand threat information sharing, including comprehensive threat assessments accompanied by mandatory reporting requirements.

8. Elevate coordination between states and federal agencies on election security, including real-time notification of security breaches and threats.

9. Provide federal funding for updating election infrastructure.

The right and ability to conduct free and fair elections transcend partisan politics.[17] At the Senate Select Intelligence Committee hearing on June 21, 2017, Sen. Mark Warner (D-VA), vice chairman of the committee, reminded those in attendance that "only with a robust and comprehensive response will we be able to protect our democratic processes from even more dramatic incursions in the future."[18] The committee's chairman, Sen. Richard Burr (R-NC), voiced a similar sentiment during the hearing, saying in reference to foreign interference, "In 2016, we were woefully unprepared to defend and respond and I'm hopeful that we will not be caught flatfooted again."[19] Finally, Sen. King declared, "[S]hame on us if we're not prepared."[20]

U.S. election systems are not equipped to handle sophisticated cyberattacks and other interference. Even in the absence of a malicious campaign, the negative consequences of this vulnerability to the strength and resiliency of U.S. democracy and government are steep. A July 2017 poll conducted by *The Hill* found that one in four Americans will consider not participating in future elections due to concerns over cybersecurity.[21] As Sen. Marco Rubio (R-FL) noted, "[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."[22]

Luckily, there are practical steps that local, state, and federal officials can take to create resilient elections and protect self-government. In the words of Sen. Burr, "Together, we can bring considerable resources to bear and keep the election system safe."[23]

9 recommendations to address vulnerabilities in U.S. election security

1. Require voter-verifiable paper ballots or records for every vote cast

Voting machines that record votes and tally them are run on software that is vulnerable to cyberintrusions.[24] Well-resourced hackers, whether funded by foreign governments or criminal syndicates, have the access, ability, and motivation to infect computerized voting machines and tallying systems across America. This can occur even if the machines are not connected to the internet. Attackers, for example, can deploy software such as Stuxnet and Brutal Kangaroo to target offline voting machines.[25]

That is why there needs to be a paper ballot—which is software independent—for every vote cast. A paper ballot offers a record of voter intent, which will exist even if voting machines are attacked and data are altered. Paper ballots or records are necessary both to conduct meaningful postelection audits able to confirm the election outcomes, and to enable post-hoc correction in the event of malfunctions or security breaches. As described by Ed Felten, professor of computer science and public affairs at Princeton University, "If there is uncertainty after an election, either because of the possibility of tampering or just the possibility of error or malfunction, a paperless system … doesn't have any way to go back to other evidence to figure out what really happened."[26] Most experts agree that paper ballots marked by the voter, either with a pen or via a ballot-marking device, are the easiest to audit.[27] Some states still deploy electronic voting machines that can produce a paper record of voters' choices on a paper roll, which voters can review. While paper-producing electronic machines can be used, they are not ideal for auditing purposes.[28]

"If there is uncertainty after an election … a paperless system … doesn't have any way to go back to other evidence to figure out what really happened."

— Ed Felten, professor at Princeton University

Fourteen states lack voter-verified paper ballots in at least some jurisdictions.[29] Put another way, roughly a quarter of the nation's voting machines do not provide paper records for votes cast.[30] In all, the Brennan Center for Justice estimates that during the 2016 general election, some 20 percent of registered Americans voted without leaving any voter-verified paper ballot or record.[31] That number of voters—20 percent of the vote—is far more than what is necessary to swing an election. According to one post-election analysis by *The Washington Post*, a mere 0.09 percent of votes effectively decided the outcome of the 2016 presidential race.[32]

States and counties using paperless touch-screen voting systems should replace them with paper ballots and optical scanners, or invest in electronic voting machines that produce voter-verified paper records. Recognizing the potential benefits of paper-ballot systems, officials in Denton County, Texas—the state's ninth-largest county—recently announced that they would be trading out the county's electronic voting machines for paper ballots after experiencing system malfunctions resulting in long lines and incorrect vote tallies during the 2016 general election.[33] Even President Trump endorses the paper ballot system, telling reporters in November 2016, "There's something really nice about the old paper-ballot system … You don't worry about hacking."[34]

Paper-ballot optical scan systems have been shown to be more cost effective than electronic voting machines.[35] In 2008, SAVE our Votes—a Maryland-based advocacy group for secure, accessible, and verifiable elections—conducted a cost analysis of Maryland's decision to convert from a paper-based system to electronic voting machine touch screens in 2004.[36] The study found that by 2008, the cost of conducting elections increased tenfold compared with only seven years prior. A number of counties that previously used optical scan systems saw their voting equipment costs skyrocket by an average of 179 percent per voter after switching to electronic touch screens.[37] Maryland has since returned to a paper-ballot system.[38] Voting systems that use electronic machines are costlier because they require more equipment. Each precinct, for

example, requires several electronic voting machines to ensure that polling places can accommodate multiple voters at once. In contrast, paper-ballot voting systems require as few as one optical scanner and one ballot-marking station per precinct to assist voters with disabilities or language barriers.

Additionally, many states allow voters to submit completed absentee ballots over the internet—via email, fax, or web portal—where there is no way for voters to confirm that the vote they cast is the same as that recorded by the county clerk's office. While most states only allow online voting for military personnel and U.S. citizens living abroad, states such as Alaska allow online voting for all absentee voters.[39] The Department of Homeland Security's Cyber Security Division "does not recommend the adoption of online voting for elections at any level of government at this time," due to concerns over voter confidentiality and the potential for vote manipulation by malicious actors.[40] One solution going forward is to require that all absentee ballots be returned by mail.

2. Replace old voting machines

Much has been written about the dismal state of voting machines.[41] In all, 42 states use voting machines that are more than a decade old, beyond the predicted 10-year lifespan of most models.[42] As noted by cybersecurity expert and co-founder and chief development officer of the Open Source Election Technology Institute Gregory Miller, "In the time we've changed our cell phones five times, the same equipment is still running our elections."[43] Outdated voting machines pose serious security risks and are susceptible to system crashes and "vote flipping," a rare occurrence whereby an individual's vote for one candidate appears on the electronic interface as a vote for a different candidate.[44] Voters in several states—including Michigan, Massachusetts, Utah, Virginia, and Illinois—reported experiencing problems with voting machines during the 2016 general election, citing machine malfunction and paper jamming, among other issues.[45]

Old voting machines are prone to hacking, as many rely on outdated computer operating systems that do not accommodate modern-day cybersecurity protections.[46] A number of voting machines in use today run on Windows XP, a Microsoft operating system first introduced in 2001 that has not been supported since 2014.[47] As described by *Wired Magazine*'s Brian Barrett, a machine running on Windows XP "is a castle with no moat, portcullis raised, doors flung open, greeting the ravaging hoards with wine spritzers and jam."[48] On June 28, 2017, hackers attending the DEF CON hacking conference in Las Vegas infiltrated and remotely hacked voting machines—some operating on Windows XP—within just 90 minutes.[49] Moreover, upkeep for outdated machines is becoming increasingly difficult, since many parts are no longer manufactured.[50] In order to obtain the parts needed, some election administrators are turning to eBay, which comes with its own security risks.[51]

Piling onto these concerns is the fact that weak chain-of-custody practices leave voting machines vulnerable to tampering. For example, an individual with only limited access can infect a machine with malicious malware and other viruses that can corrupt honest vote counts.[52] Some electronic voting machines even include accessible ports that are an open invitation to hackers, who can plug in laptops or smartphones in order to add extra votes.[53] Even with strong chain-of-custody practices, hackers can remotely infiltrate an electronic machine's operating system, and without paper-ballot records, it is impossible to know whether a hack occurred or if votes were changed.[54]

Aside from altering votes, glitches in the functionality of voting machines can sow public distrust in election outcomes and undermine the democratic process. During last year's general election, reports surfaced of votes being "flipped" during early voting in North Carolina and Nevada.[55] The NAACP sent a letter to North Carolina's board of elections on October 24 after receiving complaints that machines in five of the state's counties had flipped votes.[56]Although those who experienced problems were ultimately able to correct the error before casting their vote, two machines were removed from an early voting site in Mecklenburg County.[57]

Given the documented problems, it is imperative that election administrators replace and upgrade all voting machines and components that still use outdated operating systems to new models that meet modern standards and up-to-date cybersecurity protections. In January, Michigan announced $40 million in state funding to upgrade its optical scanning machines—many of which are between 10 and 12 years old.[58] The new machines, which the state hopes to start introducing as soon as August 2017, will not run on Windows XP.[59] Local jurisdictions—in places such as Colorado, Florida, Texas, Wisconsin, and Virginia—are also meeting the challenge posed by outdated voting systems by investing in new voting machines.[60] Ohio too is looking to update its machines, most of which were purchased between 2005 and 2006.[61] Ohio has asked county boards of elections to provide the state with an estimated price tag for new voting systems, with the hope of having new machines in place by 2019 in anticipation for the 2020 presidential election.[62]

3. Conduct robust postelection audits, which can verify that outcomes are correct

The utility of paper ballots and voter-verified paper records is only useful for ensuring that the outcome of an election is correct if election administrators commit to carrying out robust postelection audits. As previously noted, all voting machines are vulnerable to hacking and even misprogramming, which can lead to reported election outcomes that do not match the tally of actual votes cast. For example, during a March 2012 municipal election in Palm Beach County, Florida, a software error in an optical scanning machine ended with votes being allocated to the wrong candidates, resulting in the misreporting of election results.[63] The error was discovered through a postelection audit, and the results officially changed after a court-ordered public hand count of the votes.[64]

Many jurisdictions are not doing enough to conduct audits on an adequate number of ballots to ensure election accuracy and detect manipulation of vote totals caused by failing machines or hackers. According to J. Alex Halderman, a computer science and engineering professor at the University of Michigan, only New Mexico and Colorado "conduct audits that are robust enough to reliably detect cyber attacks."[65] Having participated in numerous hacking experiments on voting machines, Halderman noted, "We need to consistently and routinely check that our election results are accurate, by inspecting enough of the paper ballots to tell whether the computer results are right."[66]

Only New Mexico and Colorado "conduct audits that are robust enough to reliably detect cyber attacks."

— J. Alex Halderman, professor at the University of Michigan

Given these facts, postelection audits—which are robust enough to create strong evidence that the outcome is accurate and to correct it if it is wrong—must be conducted after every election. Importantly, election officials must be given enough time between the closing of the polls and the certification of official election results to conduct a thorough audit. "Risk-limiting" audits increase the efficiency of the auditing process by testing only the number of ballots needed to determine the accuracy of election outcomes.[67] Risk-limiting audits generally proceed by selecting an initial sample of ballots and interpreting them by hand, then determining whether the audit must expand.[68] The number of ballots in the initial sample depends on various things, including the margin of victory in the contest.[69] Elections with wide margins of victory require testing fewer ballots, while races with close margins of victory require more ballots to be tested because there is less room for error.[70] Colorado is about to become the first state to regularly conduct risk-limiting audits after elections.[71] As described by Dwight Shellman, the Colorado elections office's county support manager, "If a voting system has been maliciously altered in some way, [this audit] should give the public great assurance that we are going to know that, and we will adjust the result accordingly."[72] Risk-limiting audits offer election administrators an effective and efficient way to test the accuracy of their elections without breaking the bank.

4. Update and secure outdated voter registration systems and e-poll books

America's antiquated voter registration system threatens voter privacy and the ability of eligible voters to cast ballots that count. The Brennan Center for Justice estimates that 41 states and the District of Columbia use voter registration databases that are more than a decade old, leaving them susceptible to modern-day cyberattacks.[73] If successfully breached, hackers could alter or delete voter registration information, which in turn could result in eligible Americans being turned away at the polls or prevented from casting ballots that count.[74] Hackers could, for example, switch just a few letters in a registered voter's name without detection. In states with strict voter ID laws, eligible Americans could be prevented from voting because of discrepancies between the name listed on an official poll book and the individual's ID. In addition, by changing or deleting a registered individual's political affiliation, hackers could prevent would-be voters from participating in partisan primaries. One of the major concerns associated with

Trump's new voter fraud commission is that it could establish a centralized national voter registration database, making it easy for hackers to penetrate and exploit voter registration information. As expressed by Kentucky Secretary of State Alison Lundergan Grimes, "Coordinating a national voter registration system located in the White House is akin to handing a zip drive to Russia."[75]

The threat to voter registration systems is real. According to a DHS memo obtained by CNN, the department observed "Russian cyber actors attempting to access voter registration databases prior to the 2016 elections."[76] In August 2016, the Russian government targeted a company specializing in voter registration software, VR Systems, as part of a plan to "launch a voter registration-themed spear-phishing campaign targeting U.S. local government organizations," according to National Security Agency documents obtained by The Intercept.[77] On at least one occasion, hackers installed malware on the computer of an Arizona county election official, giving hackers access to login information that could be used to breach county voter registration databases.[78] Twenty-one counties in North Carolina use software produced by VR Systems, including Durham County, which experienced the malfunction of laptops used to confirm voter registrations across multiple precincts last year, though local officials maintain that the problem was unrelated to Russian hacking.[79] In order to ensure the accuracy and accessibility of voter registration lists during voting periods, states should establish paper-based contingency plans during early voting and on Election Day in case of system failures or hacks. For example, each local polling place should have paper copies of its voter registration lists on hand that can be consulted throughout the voting process.

There are serious privacy implications associated with breaches to voter registration databases. Voter registration lists contain myriad personal information—including names, addresses, dates of birth, driver's license numbers, political affiliations, and partial Social Security numbers—of eligible voters, which could be used by foreign or domestic foes in any number of ways.[80] A report by South Carolina's Election Commission revealed that there were nearly 150,000 attempts to penetrate the state's voter registration database on Election Day last year.[81] Moreover, *Mother Jones* has reported that 40 million voter registration records are currently being sold on the dark web.[82] To ensure voter privacy, access to voter registration databases should be strictly limited to authorized personnel, while any system alterations should be tracked and preserved.[83]

There were nearly 150,000 attempts to penetrate South Carolina's voter registration database on Election Day last year.

The widespread use of e-poll books is also a point of potential vulnerability.[84] While e-poll books, which are currently or soon will be used by 34 states and the District of Columbia, have been shown to increase efficiency and reduce wait times at polling places, they are subject to tampering and malfunction, as is true with any electronic system.[85] E-poll books should be tested prior to each election—as is currently required in at least nine states—and should only transmit information to other polling locations through secure channels, such as virtual private networks.[86] All e-poll books should be able to print a paper record that includes every person who has already checked in to

vote during early voting and on Election Day, in case of system failure. Of those states that use e-poll books and took part in a 2017 Pew Charitable Trusts survey, three—New Mexico, Colorado, and Indiana—currently lack backup paper rolls on Election Day.[87] Three other states—California, Florida, and Illinois—lack paper backups in at least some jurisdictions.[88] As with all election infrastructure, basic cybersecurity protections must be included as part of any e-poll book program. Additionally, written contingency protocol should be in place in the event of software error or suspicious discrepancies between e-poll books and paper voter lists.[89]

Finally, lawmakers should implement common-sense voter registration upgrades by enacting automatic voter registration (AVR), as has already been done in eight states and the District of Columbia.[90] AVR streamlines the election process for both voters and election officials, while making voter registration lists more accurate and secure.[91] AVR should accompany adoption of voter registration upgrades that incorporate model cybersecurity defenses. Aside from AVR, a number of states have taken steps to update their voter registration databases, soliciting bids from vendors or introducing legislation that would allocate funds for the purposes of improving voter registration systems.[92]

5. Require minimum cybersecurity standards for voter registration systems and other pieces of voting infrastructure

Experiments conducted by computer scientists on electronic voting machines have shown that they are easily hacked, can be reprogrammed to predetermine electoral outcomes and are susceptible to malicious vote-stealing software.[93] Moreover, cybersecurity vulnerabilities in voter registration systems leave the privacy and voting rights of millions of voting-eligible Americans at risk. As reported by *Politico* in June 2017, a security failure in Georgia's voter registration database, first discovered in 2016, left the voter registration records of up to 6.7 million people vulnerable to attack.[94] After discovering the system's security flaw and breaching the system, security researcher Logan Lamb alerted Kennesaw State University's Center for Election Systems, which is responsible for testing the state's touch screen voting machines and maintaining its software.[95] After being informed of the vulnerability in August 2016, the election center's executive director reportedly offered Lamb his gratitude, promising to get the server fixed.[96] Seven months later, in March 2017, the system was still vulnerable to infiltration.[97] The election center eventually brought in outside security experts and is said to have replaced its web server.[98]

Minimum cybersecurity standards for election infrastructure are sorely lacking at both the state and the federal levels. The hacking of election machines and voter registration systems is a matter of national security. States and the federal government must respond by implementing, without delay, mandatory cybersecurity standards for all election infrastructure. [99]

Some state officials are already taking affirmative steps to establish minimum cybersecurity standards to protect state systems and databases. For example, many states already have some form of cybersecurity incident and disruption response plan in place to protect against and respond to cyberthreats.[100] In addition, this past July, the National Governors Association, led by Virginia Gov. Terry McAuliffe (D), announced that 38 governors from across the country entered into "A Compact to Improve State Cybersecurity."[101] As part of the compact, states commit to "[d]eveloping a statewide cybersecurity strategy that emphasizes protecting the state's IT networks, defending critical infrastructure, building the cybersecurity workforce and enhancing private partnerships."[102] States further agree to "[c]onducting a risk assessment to identify cyber vulnerabilities, cyber threats, potential consequences of cyberattacks and resources available to mitigate such threats and consequences," among other things.[103] These efforts are a strong start, but further steps are needed to include a plan of action carefully tailored to the unique traits of voting infrastructure.

6. Perform mandatory pre-election testing on all voting machines, as well as continuous vulnerability analysis

States should conduct mandatory pre-election tests on all voting machines to ensure that they are in good working order before a single vote is cast. Most states already have laws in place requiring state officials to test voting machines and equipment in the weeks and months leading up to an election, though their scope varies depending on the jurisdiction.[104] Some states require that all voting machines be tested, while others permit the testing of a small sampling of machines.[105] And while pre-election testing may be required, it is not always carried out in practice. Admittedly, pre-election testing is not foolproof and can be manipulated, particularly by sophisticated actors.[106] That being said, pre-election testing remains an important step that states can take to mitigate machine-related problems on Election Day and protect the reliability of election outcomes.

Testing should be conducted on all election machines and equipment, including e-poll books, on multiple occasions prior to the start of early voting and Election Day. Testing should be carried out with appropriate public notice and in a public forum in an effort to increase transparency and public confidence in the electoral process. Critically, testing must be completed with enough time to allow for effective remediation. Any abnormalities should be reported immediately to officials overseeing election administration and security, and they should be shared between states, localities, and federal agencies to alert other election administrators to potential threats.

Additionally, in order to understand the full extent of election-related risk, vulnerability analysis should be carried out continuously on all election machines and voter registration databases.[107] In the words of Sen. Ron Wyden (D-OR), "We obviously need to know about vulnerabilities, so that we can find solutions."[108] Vulnerability analysis of

election infrastructure should be mandated by state and federal law and should include regular system penetration testing and vulnerability scans. Once conducted, states will be better positioned to assess where government resources should be allocated and plan for preventative measures and strategies.

Vulnerability analysis should be carried out by qualified, impartial professionals, rather than election equipment vendors or election administrators, who may have an interest in minimizing shortcomings in election machines and downplaying election vulnerabilities. States too can conduct regular vulnerability assessments on their election infrastructure. Some states—including Maryland and Washington—have employed their Air National Guard to conduct cybersecurity testing on public networks.[109] In 2016, the Ohio National Guard took part in defending the state's elections systems by running penetration tests to detect vulnerabilities and searching for evidence of malicious activity.[110] Other states, including Ohio and Virginia, have reportedly carried out security assessments on their voter registration databases, costing an estimated $25,000 and $40,000, respectively—a fraction of their annual budgets.[111] Regular, automated scans should be conducted on voter registration databases to detect suspicious activity as soon as it occurs. Suspicious findings should be reported immediately to federal agencies and to other state and local election officials around the country. The federal government could incentivize such analysis via grant programs, including those that exist at DHS, and Congress should explore whether such programs are sufficiently flexible and resourced to support these efforts.

7. Expand threat information sharing, including comprehensive threat assessments accompanied by mandatory reporting requirements

To gain an overall appreciation of the risk to our election systems, the vulnerability assessments discussed above must be matched with information sharing that includes comprehensive threat assessments. While the federal government is well-versed in providing this assistance generally, the urgent need to protect our democratic processes should be a catalyst for further reform, as Russia's interference in the 2016 election demonstrated clear stovepiping within the intelligence community (IC), and between the IC and state and local governments. For example, information-sharing organizations such as the state-run intelligence fusion centers and the Information Sharing and Analysis Centers (ISACs) have enjoyed some success, whether in the counterterrorism or the cybersecurity context.[112] But to counter foreign threats to election systems, the scope of IC support for such organizations should be expanded, while public-private sector coordination as related to critical infrastructure and cybersecurity should be appropriately leveraged.[113]

More broadly, the U.S. government should undertake reform to ensure that the whole of the intelligence community is supporting federal and state efforts to enhance election security. For example, Congress should urge the IC to prioritize collection and dissemination of information pertaining not just to cyberthreats but also to specific threats to elections and election systems, ideally through the National Intelligence Priorities Framework—which sets priorities for the entire IC—with the goal of making this intelligence shareable with state and local officials, via the FBI or DHS, in both classified and unclassified formats.[114] Another step would be for the IC to conduct a comprehensive National Intelligence Estimate concerning threats to elections and make it unclassified.[115] Finally, the newly formed Cyber Threat Intelligence Integration Center should assume a lead role in integrating various intelligence streams to give stakeholders—including policymakers, Congress, and state and local officials—a comprehensive and continuous snapshot of cyber-related election threats, be they cyberintrusions specifically or related campaigns such as influence operations.[116]

The U.S. intelligence community is best equipped to carry out threat assessments, as it has the personnel and resources necessary to thoroughly probe and analyze complex election databases, machines, and cyber vulnerabilities.[117] In carrying out these assessments, federal officers must work closely with state officials who are more familiar with the intricacies of their unique systems. State officials who have appropriate security clearances should also be provided with regular classified briefings on cybersecurity threats and system vulnerabilities.[118] All federal agencies responsible for conducting election infrastructure threat assessments should be required to submit biannual reports—classified and unclassified—to Congress on their findings, as a means of educating lawmakers and the public on threats and making recommendations for best practices.[119] In addition, Congress should receive swift notification of any intelligence concluding that there have been cyberattacks or intrusions on our election system, or evidence that a foreign adversary has sought to interfere in our democracy.

8. Elevate coordination between states and federal agencies on election security matters, including real-time notification of security breaches and threats

On January 6, 2017, the Department of Homeland Security designated election systems as "critical infrastructure," defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[120] The designation places election systems on the same level of importance as our country's financial services industry and transportation systems, and it is an important first step in protecting the future of America's elections and system of self-government.[121]

A "critical infrastructure" designation comes with benefits for election administrators, including priority status for requests submitted to DHS, domestic and international cybersecurity protections provided by federal agencies, and access to the Multi-State Information Sharing and Analysis Center (MS-ISAC).[122] MS-ISAC facilitates and provides avenues for information sharing between states and DHS, furthering the ability of states to prevent and respond to cyberattacks.[123] According to DHS, the department is already holding biweekly teleconferences with "all relevant election officials," which is a promising start.[124] However, DHS should be held accountable for specifying comprehensive, specific steps it will undertake to support this designation.[125] This may include determining whether MS-ISAC support is sufficient to meet the task or whether a more focused effort, such as the establishment of an election-focused information sharing hub, should take place.

The ability to share information and synchronize responses in real time is essential to protecting U.S. election security and resilience.[126] States and federal officials must work together, combining their expertise on cybersecurity threats and insight on the unique qualities of localized election infrastructure, to better assess and deter attempts at electoral disruption. Federal bodies and state officials are already coming together to address the issue. In July 2017, the Election Assistance Commission (EAC) in coordination with DHS, hosted a two-day meeting with election administrators and stakeholders from around the country to address threats to election infrastructure.[127] According to the EAC, the meeting involved conversations over the designation of elections as "critical infrastructure" and next steps for information sharing between interested parties.[128]

Coordinated partnership between levels of government—especially as related to voting and elections—has not always been conducted in the most efficient or effective manner. For example, some state officials voiced frustration after first learning that their state may have been one of those targeted by Russian operatives during the 2016 elections through testimony given recently by DHS officials before Congress.[129] There is room for improvement in identifying, promoting, and exercising channels for communicating key information. The See Something, Say Something campaign or the Nationwide Suspicious Activity Reporting Initiative may offer guidance to set up public education campaigns in the context of election security.[130] The private sector also has a role to play. Election vendors, for example, should be required to provide notice to states in the event that their systems are hacked, in order to prevent potential problems from arising during elections.

The role of federal agencies in protecting election security does not constitute a federal takeover of election administration. As aptly described by Sen. King of Maine, "[N]obody's talking about a federal takeover of local election systems or the federal rules. What we're talking about is technical assistance in information and perhaps some funding, at some point."[131] By designating election systems as critical infrastructure, coordination between stakeholders has the potential to be improved, but it will depend on sustained pressure and engagement by concerned stakeholders.

9. Provide federal funding for updating election infrastructure

Updating outdated election infrastructure, conducting mandatory audits, and putting in place minimum cybersecurity standards and testing is essential and requires resources. Some estimates suggest the nationwide cost of updating outdated voting machines to be upward of $1 billion, while the cost of replacing the country's paperless machines is between $130 million and $400 million.[132] At the same time, the national cost of conducting threat assessments for voter registration databases is estimated to be between $1 million and $5 million annually, with nationwide risk-limiting audits for federal elections costing less than $20 million per year, according to some evaluations.[133] According to one study conducted by the Brennan Center for Justice, of the 274 election officials surveyed in 28 states, more than half said that they will need new voting machines by 2020.[134] Unfortunately, 80 percent of those officials said they "did not have all the necessary funds."[135] State and local election administrators cannot, and should not, be expected to independently foot the bill on these protective measures. It is the responsibility of Congress to defend American interests and ensure that our elections, which are central to a functioning democracy, are free, fair, and secure. The federal government and Congress have a duty to allocate funding and assist in the implementation of measures to guard against disruptions in future elections, at the very least in federal elections.

This would not be the first time that Congress provided funds to upgrade election infrastructure. In the 2000 presidential election, antiquated punch-card voting machines resulted in thousands of lost and uncounted votes. In response, Congress passed the Help America Vote Act of 2002, providing $3 billion to help states upgrade to high-tech voting machines.[136] Congress should once again recognize the current crisis affecting U.S. elections—this time with the added threat of foreign adversaries actively seeking to infiltrate election databases and sway election outcomes.[137] It is encouraging that funding for the EAC was also recently restored, after earlier attempts to defund the agency.[138] The EAC is responsible for helping ensure the proper functioning and security of election machines, and as noted by Rep. Steny H. Hoyer (D-MD), "provides one of our strongest built-in protections against cyberattacks on our voting infrastructure."[139]

> The EAC "provides one of our strongest built-in protections against cyberattacks on our voting infrastructure."
>
> — Rep. Steny H. Hoyer (D-MD)

Congress must act now to pass legislation that, contingent upon the adoption of best practices, provides state and localities the necessary funding to:

- Upgrade outdated, insecure voting machines and voter registration systems and equip them with cybersecurity standards
- Conduct automatic post-election audits and pre-election testing on all voting machines
- Carry out comprehensive threat assessments and vulnerability analysis on voting machines and voter registration databases[140]

In addition to offsetting the cost burdens on state, county, and municipal election administrators—many of whom simply cannot afford to update and secure election machines and databases—federal funding can stem inequity resulting from uneven municipal operating budgets. When state and local jurisdictions are held solely responsible for purchasing new voting machines or providing other updates to their election systems, it is often the case that richer, majority white communities receive newer, more reliable machines and upgraded security measures.[141] Conversely, poorer communities and communities of color are left with inadequate machines and cyber protections that can lead to a higher likelihood that they may not be able to exercise their right to vote as a result of malfunctioning and easily hacked voting machines or election databases.[142] The allocation of federal funds can therefore counterbalance the unequal distribution of state and local resources to ensure that funding goes where it is most needed and to help guarantee that all Americans who are eligible to vote are able to participate in the electoral process using secure and reliable systems.

Conclusion

As it currently exists, America's election infrastructure is dangerously insecure and susceptible to hacking, machine malfunctioning, and Election Day disruption. In 2016, Russia exhibited both the skill and determination to cause problems and sow distrust in U.S. electoral processes and outcomes. It is safe to assume that Russia is right now strategizing its next plan of attack, honing its abilities to infiltrate sensitive state and federal election machines and databases without detection and to maximum effect. As Sen. Burr warned, "This adversary is determined. They're aggressive and they're getting more sophisticated by the day."[143] Failure to put in place measures and provide funding to protect election infrastructure is the height of political negligence. It is critical that we begin building our defenses to protect against election intrusions before it is too late. The future of our democracy depends on immediate action by government officials and election administrators at all levels to update and safeguard America's election systems and processes.

Danielle Root is the voting rights manager for Democracy and Government at the Center for American Progress. Liz Kennedy is the director of Democracy and Government Reform at the Center.

The authors would like to thank Marian Schneider, Moira Whelan, Susannah Goodman, and Patrick Barry for their contributions to this issue brief.

Endnotes

1 Lauren Carroll, "What we know about Russia's role in the DNC email leak," PolitiFact, July 31, 2016, available at http://www.politifact.com/truth-o-meter/article/2016/jul/31/what-we-know-about-russias-role-dnc-email-leak/.

2 Charlie Savage, "Trump campaign is sued over leaked emails linked to Russia," *The New York Times*, July 12, 2017, available at https://www.nytimes.com/2017/07/12/us/politics/trump-campaign-and-adviser-are-sued-over-leaked-emails.html?mtrref=electionlawblog.org.

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* (Executive Office of the President, 2017), available at https://www.dni.gov/files/documents/ICA_2017_01.pdf.

4 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 SNA 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/.

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

6 Ibid.

7 Tal Kopan, "DHS officials: 21 states potentially targeted by Russia hackers pre-election," CNN, July 18, 2017, available at http://www.cnn.com/2017/06/21/politics/russia-hacking-hearing-states-targeted/index.html.

8 See, for example, Matthew Rosenberg and others, "Comey Confirms F.B.I. Inquiry on Russia; Sees No Evidence of Wiretapping," *The New York Times*, March 20, 2017, available at https://www.nytimes.com/2017/03/20/us/politics/intelligence-committee-russia-donald-trump.html.

9 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/.

10 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. On file with authors. See also Beckwith, "Read the transcript of James Comey's testimony."

11 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," *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.

12 See Scott Wolchok and others, "Attacking the Washington D.C. Internet Voting System," Working Paper (16th Conference on Financial Cryptography and Data Security, 2016), available at https://jhalderm.com/pub/papers/dcvoting-fc12.pdf; Robert Cunningham, Matthew Bernhard, and J. Alex Halderman, "The Security Challenges of Online Voting Have Not Gone Away," IEEE Spectrum, November 3, 2016, available at http://spectrum.ieee.org/tech-talk/telecom/security/the-security-challenges-of-online-voting-have-not-gone-away.

13 Max Bergmann and Carolyn Kenney, "War by Other Means" (Washington: Center for American Progress, 2017), available at https://www.americanprogress.org/issues/security/reports/2017/06/06/433345/war-by-other-means/.

14 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.

15 Ibid. Since the election, two more states and six additional localities have requested assessments.

16 Transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 1."

17 As former FBI Director James Comey told the country in his June testimony before Congress, "this is about America, not about any particular party." Beckwith, "Read the transcript of James Comey's testimony."

18 Transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 1."

19 Ibid.

20 Ibid.

21 Joe Uchill, "One in four will consider not voting in elections due to cybersecurity," *The Hill*, July 12, 2017, available at http://thehill.com/policy/cybersecurity/341608-one-in-four-will-consider-not-voting-in-elections-due-to-cybersecurity.

22 Transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 1."

23 Transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 2," June 21, 2017. Provided to authors by Bloomberg Government, July 30, 2017. On file with authors.

24 See, for example, Robert Schlesinger, "Hack the Vote: a reminder of how insecure our ballots can be," *U.S. News & World Report*, July 31, 2017, available at https://www.usnews.com/opinion/thomas-jefferson-street/articles/2017-07-31/hackers-demonstrate-how-vulnerable-voting-machines-are.

25 Josephine Wolff, "Great, Now Malware Can Jump the 'Air Gap' Between Computers," *Slate*, December 3, 2013, available at http://www.slate.com/blogs/future_tense/2013/12/03/researchers_michael_hanspach_michael_goetz_prove_malware_can_jump_air_gap.html; Swati Khandelwal, "Brutal Kangaroo: CIA-developed Malware for Hacking Air-Gapped Networks Covertly," The Hacker News, June 22, 2017, available at http://thehackernews.com/2017/06/wikileaks-Brutal-Kangaroo-airgap-malware.html; Bradley Barth, "WikiLeaks: CIA's Brutal Kangaroo toolset lets malware hop onto closed networks," *SC Media*, June 22, 2017, available at https://www.scmagazine.com/wikileaks-cias-brutal-kangaroo-toolset-lets-malware-hop-onto-closed-networks/article/670395/.

26 Lily Hay Newman, "The simple fix that'd help protect Georgia from election hacks," *Wired*, June 15, 2017, available at https://www.wired.com/story/georgia-runoff-election-hack-audit-vote/.

27 See Mark Lindeman and Philip B. Stark, "A Gentle Introduction to Risk-limiting Audits," *IEEE Security and Privacy*, March 2012, available at https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

28 See Transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 2"; Ted Selker and Jon Goler, "Security vulnerabilities and problems with VVPT," Working Paper 16 (Caltech/MIT Voting Technology Project, 2004), available at https://dspace.mit.edu/bitstream/handle/1721.1/96553/vtp_wp16.pdf?sequence=1.

29 One of these states, Virginia, has been the site of several close elections over the past two decades, including the 2005 and 2009 attorney general races, decided by margins of fewer than 1,000 votes out of millions cast. Virginia's lack of adequate paper trails makes properly auditing these kinds of close elections impossible. See Kim Zetter, "Virginia finally drops America's 'worst voting machines'," *Wired*, August 17, 2015, available at https://www.wired.com/2015/08/virginia-finally-drops-americas-worst-voting-machines/; Verified Voting, "The Verifier—Voting Place Equipment—Current," available at https://www.verifiedvoting.org/verifier/ (last accessed July 2017); Lawrence Norden and Ian Vandewalker, "Securing Elections From Foreign Interference" (Washington: Brennan Center for Justice, 2017), available at https://www.brennancenter.org/publication/securing-elections-foreign-interference; Pam Fessler, "If Voting Machines Were Hacked, Would Anyone Know?", NPR, June 14, 2017, available at http://www.npr.org/2017/06/14/532824432/if-voting-machines-were-hacked-would-anyone-know.

30 Sue Halpern, "Our Hackable Democracy," *The New York Review of Books*, August 10, 2017, available at http://www.nybooks.com/daily/2017/08/10/our-hackable-democracy/.

31 Norden and Vandewalker, "Securing Elections From Foreign Interference."

32 Tim Meko and others, "How Trump won the presidency with razor-thin margins in swing states," *The Washington Post*, November 11, 2016, available at https://www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins/.

33 Emma Platoff, "Why one of the largest counties in Texas is going back to paper ballots," *Texas Tribune*, July 4, 2017, available at https://www.texastribune.org/2017/07/04/why-one-largest-counties-Texas-going-back-paper-ballots/.

34 Allan Smith, "FOX NEWS HOST TO TRUMP: 'If you do lose tonight, what is your next move?'," Business Insider, November 8, 2016, available at http://www.businessinsider.com/donald-trump-election-day-fox-news-2016-11.

35 Sarah Breitenbach, "Aging Voting Machines Cost Local, State Governments" (Washington: The Pew Charitable Trusts, 2016), available at http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2016/03/02/aging-voting-machines-cost-local-state-governments.

36 Save Our Votes, "Cost Analysis of Maryland's Electronic Voting System" (2008), available at http://www.saveourvotes.org/legislation/packet/08-costs-mdvotingsystem.pdf.

37 Ibid.

38 Pamela Wood, "Maryland ditches touch screen machines for early voting," *The Baltimore Sun*, February 4, 2016, available at http://www.baltimoresun.com/news/maryland/politics/bs-md-paper-ballots-20160204-story.html.

39 See Sari Horwitz, "More than 30 states offer online voting, but experts warn it isn't secure," *The Washington Post*, May 17, 2016, available at https://www.washingtonpost.com/news/post-nation/wp/2016/05/17/more-than-30-states-offer-online-voting-but-experts-warn-it-isnt-secure/?utm_term=.4578e3410873; National Conference of State Legislatures, "Electronic Transmission of Ballots," January 16, 2017, available at http://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx.

40 Horwitz, "More than 30 states offer online voting, but experts warn it isn't secure."

41 Laurence Norden and Christopher Famighetti, "America's Voting Machines at Risk" (Washington: Brennan Center for Justice, 2015), available at https://www.brennancenter.org/publication/americas-voting-machines-risk.

42 Ibid.; Norden and Vandewalker, "Securing Elections From Foreign Interference." These states include: Alabama; Alaska; Arizona; Arkansas; California; Colorado; Connecticut; Delaware; Florida; Georgia; Illinois; Indiana; Iowa; Kansas; Kentucky; Louisiana; Massachusetts; Michigan; Minnesota; Mississippi; Missouri; Montana; Nebraska; Nevada; New Hampshire; New Jersey; North Carolina; North Dakota; Ohio; Oregon; Pennsylvania; South Carolina; South Dakota; Tennessee; Texas; Utah; Vermont; Virginia; Washington; West Virginia; Wisconsin; and Wyoming.

43 Lauren Smiley, "America's voting machines are a disaster in the making," *New Republic*, October 19, 2016, available at https://newrepublic.com/article/137115/americas-voting-machines-disaster-making.

44 Brennan Center for Justice, "Voting System Security and Reliability Risks" (2016), available at https://www.brennancenter.org/analysis/fact-sheet-voting-system-security-and-reliability-risks; Norden and Vandewalker, "Securing Elections From Foreign Interference"; Haley Sweetland Edwards, "'Vote Flipping' Happens, But It Doesn't Mean the Election Is Rigged," *Time*, October 27, 2016, available at http://time.com/4547594/vote-flipping-election-rigged/.

45 FOX 2 Detroit, "Voting machine problems reported across metro Detroit," November 8, 2016, available at http://www.fox2detroit.com/news/elections-2016/216159836-story; Travis Anderson, "Springfield election monitors cite problems with voting machines, registration information," *The Boston Globe*, November 8, 2016, available at https://www.bostonglobe.com/metro/2016/11/08/springfield-election-monitors-cite-problems-with-voting-machines-registration-verification/7NQCmRwOqn4JYbvf29gOPJ/story.html; Georgette Braun, "Technical glitches cause minor Election Day hiccups in Rockford, Winnebago County," rrstar.com, November 8, 2016, available at http://www.rrstar.com/news/20161108/technical-glitches-cause-minor-election-day-hiccups-across-rockford-winnebago-county; Tess Owen, "Utah vote glitch," Vice News, November 8, 2016, available at https://news.vice.com/story/voting-machines-are-broken-at-every-polling-place-in-one-utah-county; Mark Berman, William Wan, and Sari Horwitz, "Voters encounter some malfunctioning machines, other headaches on Election Day," *The Washington Post*, November 8, 2016, available at https://www.washingtonpost.com/news/post-nation/wp/2016/11/08/election-day-voters-report-long-lines-intimidation-and-confusion-in-some-parts-of-the-country/?utm_term=.80fc634a57f7; Scott Wise and Claudia Rupcich, "Machine problems, long lines greet some Virginia voters," CBS 6, November 8, 2016, available at http://wtvr.com/2016/11/08/virginia-voting-issues/.

46 Norden and Vandewalker, "Securing Elections From Foreign Interference."

47 Brian Barrett, "If you still use Windows XP, prepare for the worst," *Wired*, May 14, 2017, available at https://www.wired.com/2017/05/still-use-windows-xp-prepare-worst/; Lawrence Norden, "Opinion: Protect Our Voting Machines From Hackers," NBC News, August 12, 2016, available at http://www.nbcnews.com/news/us-news/opinion-protect-our-voting-machines-hackers-n628441.

48 Barrett, "If you still use Windows XP, prepare for the worst." In May 2017, the United Kingdom ordered its National Health Service (NHS) to upgrade of all of its computer systems by February 2018, after falling victim to a ransomware attack that compromised the sensitive medical information of 200,000 people worldwide. At the time of the attack, 1 in 20 NHS machines ran on Windows XP operating systems, the same system used by many U.S. voting machines. See Laura Donnelly, "NHS ordered to upgrade outdated system as disruption continues," *The Telegraph*, May 15, 2017, available at http://www.telegraph.co.uk/news/2017/05/15/cyber-attack-nhs-ordered-upgrade-outdated-systems-disruption/.

49 Tom Porter, "Hackers breach U.S. voting machines in 90 minutes in DEF CON competition," *Newsweek*, July 30, 2017, available at http://www.newsweek.com/hackers-breach-us-voting-machines-90-minutes-def-con-competition-643858.

50 Smiley, "America's voting machines are a disaster in the making."

51 Ibid.

52 Ben Wofford, "How to Hack an Election in 7 Minutes," *Politico*, August 5, 2016, available at http://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144.

53 Machines such as the Sequoia AVC Edge possess a posterior button that allows users to submit multiple ballots. A poll worker need only press down on the button twice for several seconds and answer a prompt that places the machine into "'poll worker activation' mode." See Nsikan Akpan, "Here's how hackers might mess with electronic voting on Election Day," PBS, November 8, 2016, available at http://www.pbs.org/newshour/updates/heres-how-hackers-could-mess-with-electronic-voting/; Ian Hoffman, "Button on e-voting machine allows multiple votes," *East Bay Times*, November 1, 2006, available at http://www.eastbaytimes.com/2006/11/01/button-on-e-voting-machine-allows-multiple-votes/.

54 Porter, "Hackers breach U.S. voting machines in 90 minutes in DEF CON competition."

55 Reports of vote flipping also surfaced in Texas, but poll workers were unable to confirm the errors. See Pam Fessler, "Some Machines Are Flipping Votes, But That Doesn't Mean They're Rigged," NPR, October 26, 2017, available at http://www.npr.org/2016/10/26/499450796/some-machines-are-flipping-votes-but-that-doesnt-mean-theyre-rigged; Rollcall Staff, "Trump Asks 'What is going on' with Texas Vote Flipping," Roll Call, October 27, 2016, available at http://www.rollcall.com/news/politics/trump-texas-vote-flipping-irregularities-rigged; Marissa Kynaston, "Early Clark County voters concerned about vote flipping," KTNV, October 24, 2016, available at http://www.ktnv.com/news/political/early-voters-concerned-about-vote-flipping; Zachary Roth, "Election 2016: Tracking Reports of Voting Problems Across the United States," NBC News, November 7, 2016, available at http://www.nbcnews.com/storyline/2016-election-day/election-2016-tracking-reports-voting-problems-across-united-states-n673236.

56 Fessler, "Some Machines Are Flipping Votes, But That Doesn't Mean They're Rigged."

57 Ibid.

58 Emily Lawler, "Michigan voters may see new voting machines as soon as August," MLive.com, January 25, 2017, available at http://www.mlive.com/news/index.ssf/2017/01/michigan_voters_may_see_new_vo.html; Famighetti, "How to Protect Against Foreign Interference in Elections? Upgrade Voting Technology"; Ron French, "Michigan's aging voting machines a 'catastrophe waiting to happen'," MLive.com, March 3, 2016, available at http://www.mlive.com/politics/index.ssf/2016/03/michigans_aging_voting_machine.html; Joe Carassco Jr., "Updating Michigan's Voting Machine Technology" (Lansing, MI: Michigan Senate, 2015), available at http://www.senate.michigan.gov/sfa/publications/notes/2015notes/notesfal15jc.pdf.

59 Lawler, "Michigan voters may see new voting machines as soon as August."

60 Famighetti, "How to Protect Against Foreign Interference in Elections? Upgrade Voting Technology"; Rachel Riley, "El Paso County commissioners OK funding for new generation of election equipment," *The Gazette*, March 21, 2017, available at http://gazette.com/el-paso-county-commissioners-ok-funding-for-new-generation-of-election-equipment/article/1599424; John Chambliss, "Polk County, Fla., to Replace All Voting Machines Before Year's End," *Digital Communities*, February 21, 2017, available at http://www.govtech.com/dc/articles/Polk-County-Fla-to-Replace-All-Voting-Machines-Before-Year-End.html; RGVProud, "Court Approves Agreement to Purchase New Voting Machines for Hidalgo County," February 6, 2017, available at http://www.rgvproud.com/news/news-alerts/court-approves-agreement-to-purchase-new-voting-machines-for-hidalgo-county/650440436; Mark Schaaf, "New voting machines planned at Racine County polls," *The Journal Times*, October 9, 2016, available at http://journaltimes.com/news/local/new-voting-machines-planned-at-racine-county-polls/article_5abee6b3-1210-57bc-92d6-01dd7ba74b4a.html; Manassas, Virginia, "New Optical Scanners," available at http://www.manassascity.org/2243/New-Optical-Scanners (last accessed August 2017).

61 Darrel Rowland, "Ohio joins nationwide effort to update voting equipment," *Digital Communities*, June 27, 2017, available at http://www.govtech.com/dc/articles/Ohio-Joins-Nationwide-Effort-to-Update-Voting-Equipment-.html.

62 Ibid. Secretary of State Jon Husted has said, "I am committed to do this before my tenure as secretary of state ends (in January 2019) … This is one that has to get done. Because there will be a day somewhere, someplace where our voting equipment will fail if we don't."

63 Jaikumar Vijayan, "E-voting system awards election to wrong candidates in Florida village," Computerworld, April 3, 2012, available at http://www.computerworld.com/article/2502640/vertical-it/e-voting-system-awards-election-to-wrong-candidates-in-florida-village.html.

64 Ibid.

65 Transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 2."

66 Halderman, "Russian interference in the 2016 election"; Morgan Chalfant, "Colorado hires startup to help audit digital election results," *The Hill*, July 17, 2017, available at http://thehill.com/policy/cybersecurity/342352-colorado-hires-startup-to-help-audit-digital-election-results.

67 See Lindeman and Stark, "A Gentle Introduction to Risk-limiting Audits."

68 Ibid.

69 Ibid.

70 Ibid.

71 Eric Geller, "Colorado to require advanced post-election audits," *Politico*, July 17, 2017, available at http://www.politico.com/story/2017/07/17/colorado-post-election-audits-cybersecurity-240631.

72 Ibid.

73 Norden and Vandewalker, "Securing Elections From Foreign Interference." These states include: Alaska; Arizona; Arkansas; Connecticut; Delaware; District of Columbia; Florida; Georgia; Hawaii; Idaho; Indiana; Iowa; Kansas; Kentucky; Louisiana; Maine; Maryland; Massachusetts; Michigan; Mississippi; Missouri; Montana; Nebraska; Nevada; New Hampshire; New Jersey; New Mexico; North Carolina; Minnesota; Ohio; Oklahoma; Oregon; Pennsylvania; Rhode Island; South Carolina; South Dakota; Tennessee; Utah; Vermont; Washington; West Virginia; and Wisconsin.

74 A Republican data firm and GOP contractors reportedly leaked personal information belonging to nearly 200 million people in June 2017. See Selena Larson, "Data of almost 200 million voters leaked online by GOP analytics firm," CNN, June 19, 2017, available at http://money.cnn.com/2017/06/19/technology/voter-data-leaked-online-gop/index.html; Wesley Bruer and Evan Perez, "Officials: Hackers breach election systems in Illinois, Arizona," CNN, August 30, 2016, available at http://www.cnn.com/2016/08/29/politics/hackers-breach-illinois-arizona-election-systems/index.html.

75 Geoff Mulvihill, "Critics say vote fraud panel could create target for hackers," *StarTribune*, August 9, 2017, available at http://www.startribune.com/could-voting-fraud-panel-create-an-easy-target-for-hackers/439352233/.

76 Herb, "First on CNN: 33 states, 36 localities asked DHS for help protecting election systems."

77 Cole and others, "Top-secret SNA report details Russian hacking effort days before 2016 election." See also Ben Mathis-Lilley, "Leaked NSA Report Says Russian Hackers Targeted Voter Registration Officials in 2016 Election," *Slate*, June 5, 2017, available at http://www.slate.com/blogs/the_slatest/2017/06/05/russian_hackers_targeted_voter_registration_officials_nsa_report_says.html.

78 Robert Windrem, "Russians hacked two U.S. voter databases, officials say," NBC News, August 30, 2016, available at http://www.nbcnews.com/news/us-news/russians-hacked-two-u-s-voter-databases-say-officials-n639551.

79 See Matthew Burns, "NC elections officials investigate alleged Russian hacking efforts," WRAL, June 6, 2017, available at http://www.wral.com/nc-elections-officials-investigate-alleged-russian-hacking-efforts/16746167/; Pam Fessler, "Russian Cyberattack Targeted Elections Vendor Tied To Voting Day Disruptions," NPR, August 10, 2017, available at http://www.npr.org/2017/08/10/542634370/russian-cyberattack-targeted-elections-vendor-tied-to-voting-day-disruptions; Mark Berman, "Long lines, machine issues reported as voting gets underway," *The Washington Post*, November 8, 2016, available at https://www.washingtonpost.com/politics/2016/live-updates/general-election/real-time-updates-on-the-2016-election-voting-and-race-results/long-lines-machine-issues-reported-as-voting-gets-underway/?utm_term=.368482f73869; Cole and others, "Top-secret NSA report details Russian hacking effort days before 2016 election."

80 Transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 2."

81 Letter from the South Carolina State Election Commission to South Carolina House Oversight Committee, April 28, 2017, available at http://www.scstatehouse.gov/CommitteeInfo/HouseLegislativeOversightCommittee/AgencyWebpages/ElectionCommission/Letter%20from%20SEC%20to%20Oversight%20Subcommittee%20with%20attachments%20(April%2028,%202017).pdf; Mallory Locklear, "South Carolina hit with 150,000 Election Day hacking attempts," engadet, July 17, 2017, available at https://www.engadget.com/2017/07/17/south-carolina-150-000-election-day-hacking-attempts/.

82 The voter registrations reportedly belong to some people in Arkansas, Colorado, Connecticut, Delaware, Florida, Michigan, Ohio, Oklahoma, and Washington state. See AJ Vicens, "Someone Is Selling More Than 40 Million Voter Records on the Dark Web," *Mother Jones*, July 26, 2017, available at http://www.motherjones.com/politics/2017/07/someone-is-selling-more-than-40-million-voter-records-on-the-dark-web/.

83 U.S. Election Assistance Commission, "Checklist for Securing Voter Registration Data," available at https://www.eac.gov/assets/1/28/Checklist_Securing_VR_Data_FINAL_5.19.16.pdf (last accessed August 2017).

84 A used election poll book sold on eBay, for example, was recently found to still contain the personal information of 650,000 Tennessee voters after election officials failed to erase sensitive voter data. See Kevin Collier, "Personal Info of 650,000 Voters Discovered on Poll Machine Sold on Ebay," Gizmodo, August 1, 2017, available at http://gizmodo.com/personal-info-of-650-000-voters-discovered-on-poll-mach-1797438462?utm_campaign=socialflow_gizmodo_facebook&utm_source=gizmodo_facebook&utm_medium=socialflow.

85 Brennan Center for Justice, "VRM in the states: Electronic Poll-books," February 6, 2017, available at https://www.brennancenter.org/analysis/vrm-states-electronic-poll-books. These states include: Alabama; Arizona; Arkansas; California; Colorado; Connecticut; Florida; Georgia; Idaho; Illinois; Indiana; Iowa; Kansas; Maryland; Michigan; Minnesota; Mississippi; Missouri; Nevada; New Hampshire; New Mexico; North Carolina; North Dakota; Ohio; Pennsylvania; South Carolina; South Dakota; Tennessee; Texas; Utah; Vermont; Virginia; West Virginia; and Wyoming.

86 The Pew Charitable Trusts, "A look at how—and how many—states adopt electronic poll books," available at http://www.pewtrusts.org/en/multimedia/data-visualizations/2017/a-look-at-how-and-how-many-states-adopt-electronic-poll-books (last accessed July 2017); U.S. Election Assistance Commission, "Checklist for Securing Voter Registration Data."

87 The Pew Charitable Trusts, "A look at how—and how many—states adopt electronic poll books."

88 Ibid.

89 At least 16 states have written security protocol in place. Ibid.

90 Brennan Center for Justice, "Automatic and Permanent Voter Registration: How it Works" (2015), available at https://www.brennancenter.org/sites/default/files/publications/Automatic_Permanent_Voter_Registration_How_It_Works.pdf; National Conference of State Legislatures, "Automatic Voter Registration," available at http://www.ncsl.org/research/elections-and-campaigns/automatic-voter-registration.aspx (last accessed July 2017). These states include: Alaska; California; Colorado; Connecticut; Oregon; Rhode Island; Vermont; and West Virginia.

91 Rob Griffin and others, "Who Votes With Automatic Voter Registration" (Washington: Center for American Progress, 2017), available at https://www.americanprogress.org/issues/democracy/reports/2017/06/07/433677/votes-automatic-voter-registration/; Henry Kraemer, "Millennial Voters Win With Automatic Voter Registration" (Washington: Center for American Progress, 2017), available at https://www.americanprogress.org/issues/democracy/reports/2017/07/19/436024/millennial-voters-win-automatic-voter-registration/.

92 See Norden and Vandewalker, "Securing Elections From Foreign Interference"; Corbin Carson, "Arizona secretary of state looking to update state's voter registration systems," KTAR, May 25, 2017, available at https://ktar.com/story/1590805/1590805/; S.B. 2170 (Ill. 2017), available at http://www.ilga.gov/legislation/BillStatus.asp?DocNum=2170&GAID=14&DocTypeID=SB&LegId=106258&SessionID=91; purchase order to PCC Technology Group LLC from Texas secretary of state, July 31, 2014, available at http://www.sos.state.tx.us/about/procurement/2017-invoices/307-4-00455.pdf; State of New Jersey Department of the Treasury, "Notice of Award: Term Contract(s): T-2840," available at http://www.state.nj.us/treasury/purchase/noa/contracts/t2840_13-x-22355.shtml (last accessed August 2017); Washington State Office of the Secretary of State, "Request for Qualifications and Quotation, IT Business Analysis for Election Management System," available at https://www.sos.wa.gov/_assets/office/RFQQ%2017-08%20Work_Request.pdf (last accessed August 2017).

93 J. Alex Halderman, "Russian Interference in the 2016 U.S. Elections."

94 Kim Zetter, "Will the Georgia Special Election Get Hacked?", *Politico*, June 14, 2017, available at http://www.politico.com/magazine/story/2017/06/14/will-the-georgia-special-election-get-hacked-215255.

95 Ibid.

96 Ibid.

97 Ibid.

98 Ibid.

99 Congress has already begun putting forth legislation that would help establish cybersecurity protections for election systems. For example, Sen. Amy Klobuchar's (D-MN) Helping State and Local Governments Prevent Cyber Attacks (HACK) Act and Rep. Mark Pocan's (D-WI) Secure America's Future Elections (SAFE) Act would provide funding for securing election infrastructure. *Helping State and Local Governments Prevent Cyber Attacks (HACK) Act*, S. 1510, 115 Cong. 1 sess. (Congress.gov, 2017), available at https://www.congress.gov/bill/115th-congress/senate-bill/1510/text?q=%7B%22search%22%3A%5B%22S.1510%22%5D%7D&r=1; *SAFE Act*, H. Rept. 1562, 115 Cong. 1 sess. (Congress.gov, 2017), available at https://www.congress.gov/bill/115th-congress/house-bill/1562/text?q=%7B%22search%22%3A%5B%22H.R.1562%22%5D%7D&r=1.

100 National Governors Associations, "Meet the Threat: States Confront the Cyber Challenge: Memo on State Cybersecurity Response Plans," available at https://ci.nga.org/files/live/sites/ci/files/1617/docs/MemoOnStateCybersecurityResponsePlans.pdf (last accessed July 2017).

101 National Governors Association, "A Compact to Improve State Cybersecurity," available at https://ci.nga.org/files/live/sites/ci/files/1617/docs/1707CybersecurityCompact.pdf (last accessed July 2017); National Governors Association, "States Pledge to Meet the Cyber Threat," Press release, July 14, 2017, available at https://www.nga.org/cms/news/2017/states-pledge-to-meet-the-cyber-threat; Erin Golden, "38 Governors Sign "a Compact to Improve State Cybersecurity," *Government Technology*, July 17, 2017, available at http://www.govtech.com/policy/38-Governors-Sign-a-Compact-to-Improve-State-Cybersecurity.html.

102 National Governors Association, "A Compact to Improve State Cybersecurity."

103 Ibid.

104 See generally, Jay Bagga and others, "Pre-election logic and accuracy testing and post-election audit initiative" (Washington: Election Assistance Commission, 2013), available at https://www.eac.gov/assets/1/28/EAC%20Ball%20State%20Indiana%20Final%20Report.pdf.

105 Ibid.

106 J. Alex Halderman, "Want to Know if the Election was Hacked? Look at the Ballots," Medium, November 23, 2016, available at https://medium.com/@jhalderm/want-to-know-if-the-election-was-hacked-look-at-the-ballots-c61a6113b0ba.

107 When asked during the June 21 Senate Select Intelligence Committee hearing whether Russian operatives implanted malware or other malicious components into U.S. election systems, giving Russia easier access to voting machines and databases in future elections, Bill Priestap, assistant director of the FBI's Counterintelligence Division, declined to answer, citing impending investigations. See Transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 1."

108 Ibid.

109 According to the National Governor's Association, Maryland has made use of the state's Air National Guard 175th Network Warfare Squadron to conduct network vulnerability assessment services on state databases and systems and coordinate web-penetration training exercises with state agencies that feature simulated attacks on state websites and portals. Vulnerabilities uncovered through these exercises "lead to technical and procedural countermeasures to reduce risks." See National Governors Association, "Act and Adjust: A Call to Action for Governors for Cyber Security" (2013), available at https://www.nga.org/files/live/sites/NGA/files/pdf/2013/1309_Act_and_Adjust_Paper.pdf; Enjoli Saunders, "175th Wing activates the 175th Cyberspace Operations Group," Air National Guard, August 23, 2016, available at http://www.175wg.ang.af.mil/News/Article-Display/Article/924142/175th-wing-activates-the-175th-cyberspace-operations-group/; Washington Military Department, "October comes as #CyberAware month," available at http://mil.wa.gov/blog/news/post/were-leading-the-way-on-cybersecurity-preparedness (last accessed August 2017).

110 Rene March, "Ohio taps National Guard to defend election system from hackers," CNN, November 1, 2016, available at http://www.cnn.com/2016/11/01/politics/election-hacking-cyberattack/index.html.

111 Ohio conducted a full threat assessment, while Virginia carried out a partial assessment. Virginia officials estimate that a full assessment would cost the state $80,000 annually. See Norden and Vandewalker, "Securing Elections From Foreign Interference"; Ohio Office of Budget Management, "Actual Expenditures for FYs2012–15 and Enacted Appropriations for FYs2016–17," available at http://www.obm.ohio.gov/Budget/operating/doc/fy-16-17/FY2012-17_Expenditure_and_Appropriation_Amounts.pdf (last accessed July 2017); Virginia General Assembly, "Budget Bill—HB 30 (enrolled)," available at https://budget.lis.virginia.gov/bill/2016/1/HB30/Enrolled/ (last accessed July 2017).

112 U.S. Department of Homeland Security, "State and Major Urban Area Fusion Centers," available at https://www.dhs.gov/state-and-major-urban-area-fusion-centers (last accessed August 2017); National Council of ISACs, "About ISACs," available at https://www.nationalisacs.org/about-isacs (last accessed August 2017).

113 U.S. Department of Homeland Security, "Critical Infrastructure Sector Partnerships," available at https://www.dhs.gov/critical-infrastructure-sector-partnerships (last accessed August 2017).

114 See, for example, Homeland Security Digital Library, "ICD 204: National Intelligence Priorities Framework," available at https://www.hsdl.org/?abstract&did=761901 (last accessed August 2017).

115 Council on Foreign Relations, "National Intelligence Estimates," available at https://www.cfr.org/backgrounder/national-intelligence-estimates (last accessed August 2017).

116 Cyber Threat Intelligence Integration Center, "CTIIC Mission," available at https://www.dni.gov/index.php/ctiic-what-we-do (last accessed August 2017).

117 For example, Rep. Terri Sewell (D-AL) has introduced two bills that would strengthen cybersecurity in elections. The Securing and Heightening the Integrity of our Elections and Lawful Democracy (SHIELD) Act would require DHS to update cybersecurity at political campaign committees and share information on system vulnerabilities with committee personnel. The E-Security Fellows Act would "direct the Election Assistance Commission to establish an E-Fellows Program, training campaign staff on cybersecurity best practices." The 21st Century Voting Act—introduced by Rep. Grace Meng (D-NY)—would create a Commission on Voting tasked with, among other things, proposing legislation to strengthen and streamline election cybersecurity protections carried out by federal agencies. See Office of Congresswoman Terri Sewell, "Rep. Sewell Introduces Cybersecurity Bills to Protect Elections," Press release, July 28, 2017, available at https://sewell.house.gov/media-center/press-releases/rep-sewell-introduces-cybersecurity-bills-protect-elections; *To amend the Homeland Security Act of 2002 to secure and heighten the integrity of elections, and for other purposes*, H. Rept. 3623, 115 Cong. 1 sess. (Congress.gov, 2017), available at https://www.congress.gov/bill/115th-congress/house-bill/3623/text?q=%7B%22search%22%3A%5B%22H.R.+3623%22%5D%7D&r=1; *To direct the Election Assistance Commission to establish the E-Security Fellows Program to provide individuals who work on political campaigns with training in the best practices for election cybersecurity, and for other purposes*, H. Rept. 3622, 115 Cong. 1 sess. (Congress.gov, 2017), available at https://www.congress.gov/bill/115th-congress/house-bill/3622/text?q=%7B%22search%22%3A%5B%22H.R.+3622%22%5D%7D&r=1; *21st Century Voting Act*, H. Rept. 893, 115 Cong. 1 sess. (Congress.gov, 2017), available at https://www.congress.gov/bill/115th-congress/house-bill/893?q=%7B%22search%22%3A%5B%22H.R.+893%22%5D%7D&r=1.

118 See National Governors Association, "Act and Adjust: A Call to Action for Governors for Cyber Security."

119 For example, Rep. Sheila Jackson Lee's (D-TX) Security for the Administration of Federal Election from Terrorists Intervention (SAFETI) Act would require DHS to submit a report to the Government Accountability Office and Congress on actions it's taking relating to the integrity of the 2016 federal elections. *SAFETI Act*, H. Rept. 950, 115 Cong. 1 sess. (Congress.gov, 2017), available at https://www.congress.gov/bill/115th-congress/house-bill/950?q=%7B%22search%22%3A%5B%22H.R.+950%22%5D%7D&r=1.

120 U.S. Department of Homeland Security, "Statement by 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; 42 U.S. Code § 5195c, available at https://www.law.cornell.edu/uscode/text/42/5195c (last accessed August 2017); U.S. Election Assistance Commission, "U.S. Election Systems as Critical Infrastructure" (2017), available at https://www.eac.gov/assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf.

121 U.S. Department of Homeland Security, "Critical Infrastructure Sectors," available at https://www.dhs.gov/critical-infrastructure-sectors (last accessed July 2017).

122 Jeh Charles Johnson, "Statement before the House Permanent Select Committee on Intelligence," June 21, 2017, available at https://intelligence.house.gov/uploadedfiles/jeh_johnson_-_prepared_statement_to_hpsci_-_6-21-17_hearing.pdf; U.S. Department of Homeland Security, "Information Sharing," available at https://www.dhs.gov/topic/cybersecurity-information-sharing (last accessed July 2017).

123 U.S. Department of Homeland Security, "Information Sharing," available at https://www.dhs.gov/topic/cybersecurity-information-sharing (last accessed July 2017).

124 Transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 1."

125 For example, Rep. Hank Johnson (D-GA) introduced the Election Infrastructure and Security Promotion Act of 2017, which would require DHS to educate local election officials on the "critical infrastructure" designation and threats to our elections, among other things. *Election Infrastructure and Security Promotion Act of 2017*, H. Rept. 1907, 115 Cong. 1 sess., (Congress.gov, 2017), available at https://www.congress.gov/bill/115th-congress/house-bill/1907?q=%7B%22search%22%3A%5B%22H.R.+1907%22%5D%7D&r=1.

126 U.S. Department of Homeland Security, "Information Sharing."

127 U.S. Election Assistance Commission, "EAC Meeting Moves Election Cybersecurity Protections Forward," Press release, July 27, 2017, available at https://www.eac.gov/news/2017/07/27/eac-meeting-moves-election-cybersecurity-protections-forward/.

128 Ibid.

129 Connie Lawson, "Statement before the U.S. Senate Select Committee on Intelligence," June 21, 2017, available at https://www.intelligence.senate.gov/sites/default/files/documents/os-clawson-062117.pdf; Edward Graham, "State Officials Criticize DHS Response to Election Hacking Attempts," Morning Consult, July 18, 2017, available at https://morningconsult.com/2017/07/18/state-officials-criticize-dhs-response-election-hacking-attempts/.

130 U.S. Department of Homeland Security, "If You See Something, Say Something," available at https://www.dhs.gov/see-something-say-something (last accessed August 2017); Nationwide SAR Initiative, "About the NSI," available at https://nsi.ncirc.gov/about_nsi.aspx (last accessed August 2017).

131 Transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 1." Former Secretary of Homeland Security John Kelly said in July 2017 that states are "nuts" if they don't seek federal assistance in protecting their election systems from hackers and election inference. See Nahal Toosi, "Kelly: States 'nuts' if they don't ask feds for election protection help," *Politico*, July 19, 2017, available at http://www.politico.com/story/2017/07/19/kelly-us-elections-help-240738.

132 Lawrence Norden and Christopher Famighetti, "Now Is the Time to Replace Our Decrepit Voting Machines," Brennan Center for Justice blog, November 17, 2016, available at https://www.brennancenter.org/blog/now-time-replace-our-decrepit-voting-machines; Norden and Vandewalker, "Securing Elections From Foreign Interference."

133 Norden and Vandewalker, "Securing Elections From Foreign Interference"; Transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 2."

134 Famighetti, "How to Protect Against Foreign Interference in Elections? Upgrade Voting Technology."

135 Ibid.

136 *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; 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; Cornell Legal Information Institute, "Help America Vote Act of 2002 (HAVA): an overview," available at https://www.law.cornell.edu/background/HAVA.html (last accessed July 2017).

137 For example, Rep. Gerald Connolly's (D-VA) Fair, Accurate, Secure, and Timely (FAST) Voting Act of 2017 would provide states grants to update and secure election systems, including investing in new voting machines. *FAST Voting Act of 2017*, H. R. 1398, 115 Cong. 1 sess. (Congress.gov, 2017), available at https://www.congress.gov/bill/115th-congress/house-bill/1398/text?q=%7B%22search%22%3A%5B%22updated+election+machines%22%5D%7D&r=5.

138 Celeste Katz, "Election Assistance Commission on meeting about voting threats: 'There was a real urgency," Mic, July 28, 2017, available at https://mic.com/articles/182994/election-assistance-commission-official-on-meeting-about-voting-threats-there-was-a-real-urgency#.cpbwnDr6Y; House Appropriations Committee, "Amendment adopted to the financial services appropriations bill for FY 2018" (2017), available at https://appropriations.house.gov/uploadedfiles/all_adopted_amdts_fsgg__fy_18_-_fc_-_7-13-17.pdf.

139 U.S. Election Assistance Commission, "About the US EAC," available at https://www.eac.gov/about-the-useac/ (last accessed August 2017); Rep. Steny H. Hoyer, "Republicans Want To Defund The Commission That Fights Voting Machine Hacking," The Huffington Post, August 2, 2017, available at http://www.huffingtonpost.com/entry/5981f0e0e4b0b35d274c5f1c.

140 States could also potentially make use of grants awarded by the Federal Emergency Management Agency (FEMA) to prepare for and protect against election hacking and failure of election infrastructure. For example, Rep. Derek Kilmer's (D-WA) State Cyber Resiliency Act of 2017 would create a new State Cyber Resiliency Grant Program administered by the Federal Emergency Management Agency. *State Cyber Resiliency Act*, H. Rept. 1344, 115 Cong. 1 sess. (Congress.gov, 2017), available at https://www.congress.gov/bill/115th-congress/house-bill/1344.

141 See Norden and Famighetti, "America's Voting Machines at Risk."

142 Ibid. Virginia, Ohio, Minnesota, and Colorado counties that purchased or were in the process of purchasing new voting machines had an average median household income of at least $10,000 more than those counties that did not. See Norden *and* Famighetti, "Now Is the Time to Replace Our Decrepit Voting Machines."

143 Transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 1."