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. 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.”

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.

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. 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.

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. More requests have been made since November 2016. 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.” 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. 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.” 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.” Finally, Sen. King declared, “[S]hame on us if we’re not prepared.”

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. 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.”

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.”

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. 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.
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.” 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. 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.

Fourteen states lack voter-verified paper ballots in at least some jurisdictions. Put another way, roughly a quarter of the nation’s voting machines do not provide paper records for votes cast. 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. 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.

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. 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.”

Paper-ballot optical scan systems have been shown to be more cost effective than electronic voting machines. 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. 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. Maryland has since returned to a paper-ballot system. Voting systems that use electronic machines are costlier because they require more equipment. Each precinct, for

“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
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. 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. 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.

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. 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. 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.

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. The new machines, which the state hopes to start introducing as soon as August 2017, will not run on Windows XP. 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. Ohio too is looking to update its machines, most of which were purchased between 2005 and 2006. 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.

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. The error was discovered through a postelection audit, and the results officially changed after a court-ordered public hand count of the votes.
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.” 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.”

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. Risk-limiting audits generally proceed by selecting an initial sample of ballots and interpreting them by hand, then determining whether the audit must expand. The number of ballots in the initial sample depends on various things, including the margin of victory in the contest. 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. Colorado is about to become the first state to regularly conduct risk-limiting audits after elections. 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.” 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. 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. 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.”

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.” 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. 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. 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. 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. 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. Moreover, Mother Jones has reported that 40 million voter registration records are currently being sold on the dark web. 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.

The widespread use of e-poll books is also a point of potential vulnerability. 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. 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. All e-poll books should be able to print a paper record that includes every person who has already checked in to

There were nearly 150,000 attempts to penetrate South Carolina’s voter registration database on Election Day last year.
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 cyber threats. 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.” 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.” 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. 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. Some states require that all voting machines be tested, while others permit the testing of a small sampling of machines. 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. 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. In the words of Sen. Ron Wyden (D-OR), “We obviously need to know about vulnerabilities, so that we can find solutions.” 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. 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. 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. 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. 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.
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. Another step would be for the IC to conduct a comprehensive National Intelligence Estimate concerning threats to elections and make it unclassified. 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.

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. 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. 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. 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.” 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.
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). MS-ISAC facilitates and provides avenues for information sharing between states and DHS, furthering the ability of states to prevent and respond to cyberattacks. According to DHS, the department is already holding biweekly teleconferences with “all relevant election officials,” which is a promising start. However, DHS should be held accountable for specifying comprehensive, specific steps it will undertake to support this designation. 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. 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. 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.

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. 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. 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.” 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. 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. 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. Unfortunately, 80 percent of those officials said they “did not have all the necessary funds.” 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. 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. It is encouraging that funding for the EAC was also recently restored, after earlier attempts to defund the agency. 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.”

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

The EAC “provides one of our strongest built-in protections against cyberattacks on our voting infrastructure.”

— Rep. Steny H. Hoyer (D-MD)
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. 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. 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.” 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


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

6 Ibid.


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.”


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.


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


31 Norden and Vandewalker, “Securing Elections From Foreign Interference.”


37 Ibid.


40 Horowitz, “More than 30 states offer online voting, but experts warn it isn’t secure.”


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.


46 Norden and Vandewalker, “Securing Elections From Foreign Interference.”


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 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 systems as disruption continues,” The Telegraph, May 15, 2017, available at https://www.telegraph.co.uk/news/2017/05/15/cyber-attack-nhs-ordered-upgrade-outdated-systems-disruption/.


50 Smiley, “America’s voting machines are a disaster in the making.”
51 Ibid.


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


56 Fessler, “Some Machines Are Flipping Votes, But That Doesn’t Mean They’re Rigged.”

57 Ibid.


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


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, somewhere where our voting equipment will fail if we don’t.”


64 Ibid.

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


68 Ibid.

69 Ibid.

70 Ibid.


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; Minnesota; 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.


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

80 Transcript of “Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 2.”
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-voter-discovered-on-poll-mach-1797484627&utm_campaign=socialflow_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.


103. Ibid.


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/jahalderman/want-to-know-if-the-election-was-hacked-look-at-the-ballots-cf1ad613b0ba.

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.


14. Transcript of “Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 1.”


18. Ibid.


25. Famighetti, “How to Protect Against Foreign Interference in Elections? Upgrade Voting Technology.”

26. Ibid.


31. See Norden and Famighetti, “America’s Voting Machines at Risk.”

32. 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.”

33. Transcript of “Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 1.”

34. Famighetti, “Now Is the Time to Replace Our Decrepit Voting Machines.”

35. Ibid.