POLICY REPORT

BRENNAN CENTER FOR JUSTICE

A Framework for Election Vendor Oversight

Safeguarding America's Election Systems

By Lawrence Norden, Christopher R. Deluzio, and Gowri Ramachandran PUBLISHED NOVEMBER 12, 2019

Brennan Center for Justice at New York University School of Law

Table of Contents

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that works to reform, revitalize — and when necessary defend — our country's systems of democracy and justice. The Brennan Center is dedicated to protecting the rule of law and the values of constitutional democracy. We focus on voting rights, campaign finance reform, ending mass incarceration, and preserving our liberties while also maintaining our national security. Part think tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, in the courts, and in the court of public opinion.

ABOUT THE BRENNAN CENTER'S DEMOCRACY PROGRAM

The Brennan Center's Democracy Program encourages broad citizen participation by promoting voting and campaign finance reform. We work to secure fair courts and to advance a First Amendment jurisprudence that puts the rights of citizens — not special interests — at the center of our democracy. We collaborate with grassroots groups, advocacy organizations, and government officials to eliminate the obstacles to an effective democracy.

STAY CONNECTED TO THE BRENNAN CENTER

Visit our website at
www.brennancenter.org

Executive Summary

More than 80 percent of voting systems in use today are under the purview of three vendors.[1] A successful cyberattack against any of these companies could have devastating consequences for elections in vast swaths of the country. Other systems that are essential for free and fair elections, such as voter registration databases and electronic pollbooks, are also supplied and serviced by private companies.

Yet these vendors, unlike those in other sectors that the federal government has designated as critical infrastructure, receive little or no federal review. This leaves American elections vulnerable to attack. To address this, the Brennan Center for Justice proposes a new framework for oversight that includes the following:

- **Independent oversight.** A new federal certification program should be empowered to issue standards and enforce vendors' compliance. The Election Assistance Commission (EAC) is the most logical agency to take on the role. Unfortunately, from its founding, the EAC has had a history of controversy and inaction in carrying out its core mission. In this paper, we assume that the EAC would be charged with overseeing the new program, and we make a number of recommendations for strengthening the agency so that it could take on these additional responsibilities. Whichever agency takes on this role must be structured to be independent of partisan political manipulation, fully staffed with leaders who recognize the importance of vendor oversight, and supported by enough competent professionals and experts to do the job.
- **Issuance of vendor best practices.** Congress should reconstitute the EAC's Technical Guidelines Development Committee (TGDC) to include members with more cybersecurity expertise and empower it to issue best practices for election vendors. (The TGDC already recommends technical guidelines for voting systems.) At the very least, these best practices should encourage election vendors to attest that their conduct meets certain standards concerning cybersecurity, personnel, disclosure of ownership and foreign control, incident reporting, and supply chain integrity. Given the EAC's past failures to act on the TGDC's recommendations in a timely manner, we recommend providing a deadline for action. If the EAC does not meet that deadline, the guidelines should automatically go into effect.
- **Vendor certification.** To provide vendors a sufficient incentive to comply with best practices, Congress should expand the EAC's existing voluntary certification and registration power to include election vendors and their various products. This expanded authority would complement, and not replace, the current voluntary federal certification of voting systems, on which ballots are cast and counted. Certification should be administered by the EAC's existing Testing and Certification Division, which would require additional personnel.
- **Ongoing review.** In its expanded oversight role, the EAC should task its Testing and Certification Division with assessing vendors' ongoing compliance with certification standards. The division should continually monitor vendors' quality and configuration management practices, manufacturing and software development processes, and security postures through site visits, penetration testing, and cybersecurity audits performed by certified independent third parties. All certified vendors should be required to report any changes to the information provided during initial certification, as well as any cybersecurity incidents, to the EAC and all other relevant agencies.
- **Enforcement of guidelines.** There must be a clear protocol for addressing violations of federal guidelines by election vendors.

Congressional authorization is needed for some but not all elements of our proposal. The EAC does not currently have the statutory authority to certify most election vendors, including those that sell and service some of the most critical infrastructure, such as voter registration databases, electronic pollbooks, and election night reporting systems. For this reason, Congress must act in order for the EAC or other federal agency to adopt the full set of recommendations in this report.[2] Regardless, the EAC could, without any additional legislation, issue voluntary guidance for election vendors and take many of the steps recommended in this paper as they relate to voting system vendors. Specifically, it is our legal judgment that the EAC may require, through its registration process, that voting system vendors provide key information relevant to cybersecurity best practices, personnel policies, and foreign control. Furthermore, the EAC may deny or suspend registration based on noncompliance with standards and criteria that it publishes.

Ultimately, the best course of action would be for Congress to create a uniform framework for election vendors that adopts each of the elements discussed in this paper. In the short run, however, we urge the EAC to take the steps it can now to more thoroughly assess voting system vendors.

Introduction

The unprecedented attacks on America's elections in 2016, and repeated warnings by the country's intelligence agencies of future foreign interference, have raised the profile of election security in a way few could have imagined just a few years ago. The response has largely focused on improving the testing of voting machines before they are purchased and on training state and local election officials to institute best practices to prevent, detect, and recover from cyberattacks.

Yet private vendors, not election officials, build and maintain much of our election infrastructure. They create election websites that help voters determine how to register and where to vote; print and design ballots; configure voting machines; and build and maintain voter registration databases, voting machines, and electronic pollbooks. Not every jurisdiction outsources all of these functions, but all rely on vendors for some of this work and many for nearly all of it. Understandably, many local governments under fiscal pressure would rather contract out these functions than increase their election office staff, especially considering the cyclical nature of election-related work.

There is almost no federal regulation of the vendors that design and maintain the systems that allow us to determine who can vote, how they vote, or how their votes are counted and reported. While voting systems are subject to some functional requirements under a voluntary federal testing and certification regime, the vendors themselves are largely free from federal oversight.

This is not the case in other sectors that the federal government has designated as critical infrastructure. Vendors in the defense sector, for example, face substantial oversight and must comply with various requirements, including rules governing the handling of classified information and supply chain integrity. The federal government regulates colored pencils, which are subject to mandatory standards promulgated by the Consumer Product Safety Commission, more stringently than it does America's election infrastructure.[3]

There is a growing bipartisan appreciation that federal action is needed to address the risks that vendors might introduce into election infrastructure. Rep. Zoe Lofgren (D–CA), who chairs the Committee on House Administration, has said that a significant election-related "vulnerability comes from election technology vendors . . . who have little financial incentive to prioritize election security and are not subject to regulations requiring them to use cyber security best practices."[4] Alabama's Republican secretary of state, John Merrill, has called for the EAC to undertake "a centralized effort to evaluate the effectiveness of election equipment, whether it be for voter administration purposes, electronic poll books," or the like.[5]

While state and local governments retain primacy in running elections, only the federal government has the resources and constitutional responsibility to ensure that the more than 8,000 local election jurisdictions have access to information and expertise to safeguard federal elections from insecure vendor practices.[6] The ability of a foreign power to exploit the vulnerabilities of a vendor in a single county in Pennsylvania could have extraordinary repercussions for the country.

Given the lack of federal oversight, the relatively small number of vendors with significant market share,[7] and

Vendor Involvement in Elections

>> Voter Registration Database
Voter registration information is housed in statewide databases that in many jurisdictions are created or maintained by a vendor.

>> Ballot Programming
Prior to every election, voting machines must be programmed with a memory card or USB stick to display the ballot or read and count votes. Vendors often provide the software.

>> Electronic Pollbooks
On Election Day, poll workers in most jurisdictions check voters in using electronic pollbooks, which are usually provided by a vendor.

>> Voting Systems
Jurisdictions use a variety of voting machines, all provided by vendors.

>> Election Night Reporting
On election night, the general public can view election results through reporting websites that are often provided by vendors.

>> Postelection Audits
After an election, vendors and their equipment play a role in checking that the equipment and procedures used to count votes worked properly and that the election yielded the correct results.

their "severe underinvestment in cybersecurity,"[8] the Brennan Center proposes that the federal government take on a more substantial oversight role. Under our proposal, the EAC would extend its existing certification regime from voting systems to include all vendors that manufacture or service key parts of the nation's election infrastructure. The commission would also continuously monitor vendors, with the power to revoke certification. (The EAC currently has that power but only uses it to oversee the systems themselves.)

Definition of Election Vendor

This paper refers to "election vendors" when discussing those entities that provide election services to jurisdictions throughout the United States. A 2017 University of Pennsylvania report on the election technology industry described these entities as those "that design, manufacture, integrate, and support voting machines and the associated technological infrastructure."[9] While the report focused largely on voting systems, quantifying the sector's annual revenue at $300 million,[10] the election vendors referred to also include those that do not participate in the voting systems market but provide other election-related goods and services. For the purposes of this paper, "vendor" is defined to include any private individual or business that manufactures, sells, programs, or maintains machines that assist in the casting or tallying of votes, voter registration databases, electronic pollbooks, or election night reporting systems.

Vendors Present Points of Attack into Election Infrastructure

Private vendors' central role in American elections makes them prime targets for adversaries. Yet it is impossible to assess the precise level of risk associated with vendors — or how that risk impacts election security. As a 2018 U.S. Senate Intelligence Committee report observed, "State local, territorial, tribal, and federal government authorities have very little insight into the cyber security practices of [election] vendors."[11]

This limited visibility into vendors includes

- vendor cybersecurity practices (how vendors protect their own information technology infrastructure and data);
- foreign ownership of vendors (whether foreign nationals, or agents of foreign governments, own companies performing critical election functions);
- personnel policies and procedures (whether background checks and other procedures are in place to safeguard against inside attacks);
- cybersecurity incident response (how vendors alert relevant authorities of attacks); and
- supply chains (where parts, software patches, and installations come from; how are they transported; and how they are kept secure).

Revelations that Russian actors targeted an election vendor in the lead-up to the 2016 election provide a useful example of how little insight there is into vendor security.

Special Counsel Robert Mueller's report to the attorney general and indictment of 12 Russian intelligence officers both included allegations that these officers hacked a private U.S. elections systems vendor. The vendor is believed to operate in at least eight states, including the battleground states of North Carolina, Virginia, and Florida.[12]

According to the special counsel, hackers gained access to the vendor's computers and used an email account designed to look like the vendor's to send spearphishing emails to Florida election officials.[13] Per the indictment, "the spearphishing emails contained malware that the Conspirators embedded into Word documents bearing [the vendor's] logo."[14] According to Florida Governor Ron DeSantis, the hackers breached the election systems of two Florida counties.[15]

We still don't know all the facts. Even in the rare instance that the public learns of a vendor hack — as it did through the special counsel's investigation — many questions remain unanswered. When and how did the vendor learn of these attacks? What preventive measures were in place? What steps did the vendor take after discovering it was targeted to ensure that it was not infiltrated? Did it immediately inform its customers? The public generally never learns the answers to these questions, and there are no federal laws or regulations requiring private vendors to take any action in the event of a cyberattack.

Similarly, *Vice* recently reported that election night reporting systems sold by Election Systems and Software (ES&S), the country's leading election vendor, had been exposed to the public internet, potentially for years on end. (ES&S denied the substance and significance of the report.) Although ES&S voting machines are certified by the EAC, its transmission configuration is not.[16]

The lack of visibility into vendors and their cybersecurity can also contribute to an inability to detect poor practices that might affect vendor performance until it is too late. In 2017, ES&S left the sensitive personal information of 1.8 million Chicago voters publicly exposed on an Amazon cloud server.[17] That information reportedly

included "addresses, birth dates and partial Social Security numbers,"[18] information valuable to hackers.

Opaque supply chains further exacerbate the problem. Earlier this year, an IBM Security Services investigation on behalf of Los Angeles County found that compatibility issues between the voter list and an ES&S subsidiary's software contributed to nearly 120,000 voters being left out of printed pollbooks and forced to request provisional ballots.[19]

Although the EAC can conduct manufacturing site visits through its Quality Monitoring Program,[20] this program extends only to voting systems that are submitted for voluntary certification and does not cover the full menu of vendor products and services. There is no federal scrutiny of supply chains for components sourced for noncertified products and services, for example, despite the finding of the Department of Homeland Security (DHS) that "contractors, sub-contractors, and suppliers at all tiers of the supply chain are under constant attack."[21]

The recent ban on certain technologies made by the Chinese company Huawei is a stark illustration of the growing recognition of supply chain risk.[22] Vendors' use of local or regional partners or subcontractors adds to the lack of visibility. For instance, Unisyn Voting Solution, a digital scan voting system manufacturer whose systems have been certified by the EAC, identifies a range of partners in several states on its website.[23] Neither Unisyn nor these partners are currently subject to the kind of oversight we recommend.

Election officials often depend on vendors whose practices are opaque. Yet these companies — unlike those in other critical infrastructure sectors, such as defense, nuclear, dams, and energy — face almost no federal oversight of their security systems. There are no requirements that vendors report breaches, screen employees' backgrounds, patch security flaws, report foreign ownership or control, or ensure the physical security of sensitive software and hardware.

> The ability of a foreign power to exploit the vulnerabilities of a vendor in **a single county in Pennsylvania** could have extraordinary repercussions.

Independent Federal Oversight

This paper assumes that the Election Assistance Commission would be the agency charged with overseeing election vendors. There are many reasons why the EAC is the most logical choice for this role. One among them is that the EAC already certifies voting equipment and issues voluntary guidance. Because it is structured as an independent agency with bipartisan membership, it faces less risk of undue political meddling in the technical work of overseeing election vendors than a traditional executive agency would. Its structure could also help avoid dramatic shifts in oversight approaches with a change of presidential administrations.[24]

Unfortunately, the EAC has been plagued by controversy for years. Its leaders have waded into contentious issues, such as voter identification and proof of citizenship, that have little relation to the agency's core responsibilities.[25] It has missed deadlines for completing critical functions, such as adopting voting system guidelines.[26] And there are concerns that it has not taken election security seriously enough,[27] as well as "complaints of infighting, high [staff] turnover and cratering morale."[28]

If the EAC were chosen for this role, Congress would need to take a number of actions to make its success more likely. First, it would need to increase the agency's budget. The new role would constitute a major expansion of the EAC's regulatory mandate. In recent years, despite the increased threat of cyberattacks against our nation's election infrastructure, funding for the EAC has dropped sharply. The agency's budget in fiscal year 2019 was just $9.2 million, down from $18 million in fiscal year 2010.[29]

With expanded oversight authority, the EAC would need to dramatically increase its cybersecurity competency and knowledge. To facilitate this increased technical focus, we outline below how the existing Technical Guidelines Development Committee would need to be modified to emphasize technical proficiency and, specifically, cybersecurity expertise. We also recommend greater deference to this modified technical committee, permitting its recommended voluntary guidelines to take effect absent overriding action by the EAC. These changes, too, would require congressional action.

On the personnel front, Congress would need to commit to keeping EAC seats filled by leaders who are dedicated to working with each other and with career staff to ensure the security of our election infrastructure. Congress's failure to replace commissioners left the EAC without a quorum between December 2010 and December 2014 and then again between March 2018 and February 2019.

Finally, given the breadth and scope of this new mandate, Congress would need to subject the agency to more scrutiny and oversight than it has in the past.[30]

If Congress is unable or unwilling to take these steps, it should find a different agency to oversee election vendor certification. Any agency placed in that role must be structured so as to remain independent of partisan control. It will need experienced, effective staff and leadership who are committed to election security, cybersecurity, technical competency, and good and effective election administration.

How to Expand Voting System Vendor Registration without Legislation

Most of the policies suggested in this report will require congressional authorization. Not least of these is the ability of the Election Assistance Commission's regulatory authority to reach election system vendors for products and services other than voting machines — including voter registration databases, electronic pollbooks and election night reporting. However, the EAC can under its current authority institute a voluntary system of oversight of the security practices of vendors that supply voting systems, using a combination of its registration and certification schemes.

In order to register, voting system vendors must already provide the EAC with critical information about their ownership, along with written policies regarding their quality assurance mechanisms. Vendors must agree to certain program requirements, and registrants can be suspended if they fail to continue to abide by the registration requirements. A system cannot be submitted for certification unless its manufacturer is currently registered with the EAC.[i] The need for this type of information is clear: in order to carry out its certification, decertification, and recertification authority, including the provision of a fair process to vendors who risk decertification or denial of certification, the EAC must be able to maintain communication with voting system vendors and ensure compliance with quality assurance mechanisms on an ongoing basis.

To ensure that certified voting systems are secure, the EAC can adopt Voluntary Voting System Guidelines (VVSG) that outline best practices for vendors as they relate to cybersecurity, personnel, foreign control, and supply chain integrity. Voting system vendors can then be required, as part of registration, to provide information on their compliance with these standards.

For instance, the current VVSG provide special guidelines for voting systems that use public telecommunications networks in order to ensure that they are protected against external threats, including monitoring requirements. Similarly, the guidelines require verification methods for both software setup and any software update packages.[ii] New guidelines could outline why background checks for personnel are necessary to ensure the ongoing security of voting systems, including upgrades and changes.[iii]

The current registration process could also allow the EAC to ensure that various voting system vendor best practices remain in force over time. The process imposes a continuing responsibility on vendors to report any changes in the information supplied to the EAC and to "operate . . . consistent with the procedural requirements" established by the EAC's testing and certification manual. Thus, if registration mandated, for example, the provision of cybersecurity information from vendors, they would be required to report cybersecurity changes or incidents pursuant to their responsibility to keep registration information up to date. Registration could be suspended if vendors failed to maintain policies consistent with the EAC's requirements.[iv]

While expanding oversight of voting system vendors to ensure compliance with the basic security measures discussed in this paper would not be a substitute for a full certification system for all election system vendors, it would be a significant step toward providing greater accountability for voting system vendors.

A New Framework for Election Vendor Oversight

Under the Brennan Center's proposal, the Election Assistance Commission's oversight role would be substantially expanded. Oversight would extend beyond voting equipment[31] to election vendors themselves. The current voting system testing is intentionally quite limited: it occurs at the end of the design, development, and manufacture of voting system equipment. It does not ensure that the vendors have engaged in best supply chain or cybersecurity practices when developing equipment or when servicing or programming it once it is certified.[32] Nor does the system ensure that the vendor has conducted background checks on employees or set up controls limiting access to sensitive information.

Despite its limitations, the EAC's Testing and Certification Program — a voluntary program that certifies and decertifies voting system hardware and software — provides a good template for a vendor oversight program. A variety of bills, including the Election Security Assistance Act proposed by Rep. Rodney Davis (R–IL) and the Democratic-sponsored SAFE Act and For the People Act, have called for electronic pollbooks, which are not currently considered voting systems and covered by the program, to be included in its hardware and software testing regime.[33]

Currently, the Technical Guidelines Development Committee, a committee of experts appointed jointly by the National Institute of Standards and Technology (NIST) and the EAC, sets certification standards for voting systems. These guidelines, known as the Voluntary Voting System Guidelines (VVSG), can be adopted, with modifications, by a majority of EAC commissioners. Once approved, they become the standards against which voting machines are tested for federal certification. The VVSG ensures that voting systems have the basic functionality, accessibility, and security capabilities required by the Help America Vote Act (HAVA).[34]

Future iterations of the VVSG and certification process may change slightly: commissioners have suggested that they may support a new version of the VVSG that adopts high-level principles and guidelines for the commission to approve, along with a more granular set of certification requirements, which staff could adjust from time to time.[35]

Once new voting system guidelines are adopted, the EAC's Testing and Certification Division tests the systems (per the VVSG), certifies them, monitors them, and, if critical problems are later discovered, decertifies them. The EAC conducts field tests of voting machines only if invited or given permission by a state election official. It does not do this on a routine basis.[36] Rather, election officials using the certified voting machines have the option to report system anomalies to the EAC. If the EAC deems a report credible, it may begin a formal investigation and work with the vendor to address the problem. If the vendor fails to fix the anomaly, the EAC is obligated to decertify the voting system.[37]

With some important modifications, we recommend a similar regime for certifying election system vendors. The commissioners should adopt a set of principles and guidelines for vendors recommended by a Technical Guidelines Development Committee, as well as a more detailed set of requirements that could be adjusted as needed by EAC staff. We recommend that the EAC routinely monitor certified vendors to ensure ongoing compliance and establish a process for addressing violations of federal standards, including through decertification.

A Voluntary Regime

Federal certification will only be meaningful if state and local governments that contract with election system vendors rely on it when making purchasing decisions.

For this reason, some have recommended that state and local governments be required to use only vendors that have been federally certified. For instance, the Election Vendor Security Act proposes that state and local election administrators be banned from using any vendor for federal elections that does not meet some minimum standards.[38]

There are obvious benefits to a mandatory regime. Most important, it would ensure that all jurisdictions throughout the country use vendors that have met minimum security standards. But there are drawbacks as well. Not least of these is that some states and localities might view a federal mandate to use certain vendors as a usurpation of their power to oversee their own elections, making the creation of a federal program politically challenging.

Moreover, since private vendors are so deeply entwined in the running of our elections, requiring towns, counties, and states to use only certified vendors could present problems. If a vendor failed the certification process (or decided not to apply for certification), some counties would not be able to run their elections. Others might be forced to spend tens of millions of dollars to purchase

new equipment and services before they could run elections again, even if they had determined that they could have run their elections securely.

A voluntary approach — leaving it to the states and local jurisdictions to decide whether to contract with non–federally certified vendors — could draw states into the voting system certification process. It may also be more politically feasible. A voluntary approach would give state and local jurisdictions the flexibility to take additional security measures if their current vendors did not obtain federal certification. In selecting new vendors, most states and local election officials would likely rely on federal certification in making purchases, as they do with voting machines. Democrats in Congress opted for this approach in the For the People Act and the SAFE Act. Both measures would incentivize participation by providing grants to states that acquire goods and services from qualified election infrastructure vendors or implement other voting system security improvements.[39]

The drawback of a voluntary program is that states and vendors may ignore it. But there is reason to believe that there would be wide participation in a voluntary federal program. Even though the current voting machine certification program is voluntary, 47 of 50 states rely on the EAC's certification process for voting machines in some way.[40] Another voluntary program, DHS's Election Infrastructure Sector Coordinating Council, was founded in 2018 to share information among election system vendors. Numerous major election vendors have supported it as organizing members.[41]

Guidelines Developed by an Empowered, More Technical Committee

A new Technical Guidelines Development Committee, with additional cybersecurity experts, should be charged with crafting vendor certification guidelines for use by the Election Assistance Commission, incorporating best practices that election vendors must meet. These guidelines should go into effect unless the EAC overrides the recommendation within a specified period of time. This deference to the technically expert TGDC in the absence of an override by policymakers is necessary to avoid the kinds of lengthy delays that have stood in the way of prior attempts to update the VVSG.[42] The NIST cybersecurity framework should be the starting point for these best practices, and the TGDC need only apply election-specific refinements to this existing framework.

The TGDC is chaired by the director of the NIST. Its 14 other members are appointed jointly by the director and the EAC.[43] We recommend that Congress authorize NIST to expand TGDC's membership to include the wider range of expertise necessary to fulfill its role in defining vendor best practices. These new members should explicitly be required to have cybersecurity expertise. Congress should also mandate that a representative from the new DHS Cybersecurity and Infrastructure Security Agency (CISA), a leading voice in cybersecurity defense, including in the elections sector, join the TGDC. The Vendor System Cyber Security Act of 2019, introduced by Sen. Gary Peters (D–MI), would require this step.[44] Similarly, Congress should mandate the inclusion of a representative from the National Association of State Chief Information Officers (NACIO) with expertise in cybersecurity.[45]

Reconstituting the TGDC in this manner would not only ensure that it has the relevant expertise to set guidelines for vendors but also that there are more members with technical backgrounds.

As noted above, we recommend permitting the guidelines developed by the TGDC to take effect in the event that the EAC fails to act on them within a specified time period. We also recommend that vendors seeking certification must always meet the most recent set of guidelines. This, along with the expanded membership of the TGDC, will provide the necessary assurance that best practices are updated in a timely fashion and that vendors seeking certification meet the most up-to-date standards.[46]

The new TGDC will be responsible for developing federal certification guidelines that vendors must satisfy to sell key election infrastructure and services for use in federal elections. Areas that should be covered in such guidelines include

- cybersecurity best practices,
- background checks and other security measures for personnel,
- transparent ownership,
- processes for reporting cyber incidents, and
- supply chain integrity.

Below, we discuss the importance of each of these items, what guidelines in each of these areas could look like, and how to ensure compliance.

CYBERSECURITY BEST PRACTICES

The lead-up to the 2016 presidential election provided numerous examples of the devastating consequences of failing to heed cybersecurity best practices. Through a series of attacks that included spearphishing emails, Russian hackers gained access to internal communications of the Democratic National Committee (DNC).[47] The DNC reportedly did not install a "robust set of monitoring tools" to identify and isolate spearphishing emails on its network until April 2016, which, in retrospect, was far too late.[48] The chairman of Hillary Clinton's campaign,

John Podesta, fell prey to a similar attack.[49] These threats did not end in 2016; in the run-up to the 2018 elections, hackers targeted congressional candidates including Sen. Claire McCaskill (D–MO) and Hans Keirstead, who ran in a Democratic Party primary in California.[50]

Guarding against spearphishing emails is Cybersecurity 101. Yet the numerous reports of successful spearphishing attacks suggest that many individuals and organizations fail to meet even that low bar of cyber readiness. Are vendors guarding against these (and other) attacks?[51] Special Counsel Robert Mueller's report on 2016 election interference indicates that an employee at an election vendor fell victim to a spearphishing attack, enabling malware to be installed on that vendor's network. The vendor, which many assume is VR Systems, has denied that that the attackers were able to breach its system.[52] Under the current regime, which lacks any meaningful visibility into vendors' cybersecurity practices, we simply do not, and cannot, know.

The new Technical Guidelines Development Committee should craft cybersecurity best practices that include not only equipment- and service-related offerings but also internal information technology practices, cyber hygiene, data access controls, and the like. Various bills have proposed that the TGDC take on this role, including the SAFE Act, the Election Security Act, and the For the People Act.[53]

The NIST Cybersecurity Framework[54] should be the starting point and be supplemented by election-specific refinements. NIST advises that "the Framework should not be implemented as an un-customized checklist or a one-size-fits-all approach for all critical infrastructure organizations. . . . [It] should be customized by different sectors and individual organizations to best suit their risks, situations, and needs."[55]

When seeking Election Assistance Commission certification, vendors should have to demonstrate that they meet the TGDC's cybersecurity best practices. The EAC should consider providing a self-assessment handbook or other form of guidance to facilitate vendor compliance with this requirement.

Such a self-assessment handbook exists in the defense sector for contractors that handle certain sensitive information. Department of Defense contractors "that process, store or transmit Controlled Unclassified Information must meet the Defense Federal Acquisition Regulation Supplement minimum security standards" and certify that they comply with published requirements.[56] An EAC resource along these lines would provide vendors with clarity about how to assess compliance and agreed-upon metrics.

Similarly, DHS has published resources associated with its Cyber Resilience Review program, which "align[s] closely with the Cybersecurity Framework . . . developed by the National Institute of Standards and Technology."[57] They include a self-assessment package and a "Question Set with Guidance,"[58] which could prove useful in developing analogous resources for the EAC.

BACKGROUND CHECKS AND OTHER SECURITY MEASURES FOR PERSONNEL

Much of the conversation about election cybersecurity has imagined attackers in distant lands reaching our election infrastructure through the internet. But some of the most effective cyberattacks of recent years have involved insiders. To mitigate these risks, vendors should demonstrate during certification that they have sound personnel policies and practices in place.

At a minimum, vendors should describe how they screen prospective employees for security risks, including background checks, and how they assess employees for suitability on an ongoing basis, including substance-abuse screening. The Election Assistance Commission should also require vendor disclosure of controls governing staff access to sensitive election-related information. Since the bulk of such sensitive information would presumably not constitute classified information, which is subject to its own set of robust controls, the EAC's scrutiny of vendor personnel risk management will be critical.

> Vulnerability to attacks by insiders is a threat **separate and apart** from a hack over the internet.

Vulnerability to attacks by insiders is a threat separate and apart from a hack over the internet, demanding entirely different controls and defensive measures. Without adequate personnel screening and other safeguards, vendors that provide critical election services could be exposed to malfeasance from within. The FBI's thorough background checks for Justice Department attorneys and other law enforcement personnel provide a good model for aggressively vetting personnel. In the event election vendors require access to formally classified information, examples abound in the defense, nuclear, and other sectors of how to handle security clearances.

The Nuclear Regulatory Commission (NRC) regulates personnel in ways potentially relevant to election vendors.[59] Its fitness-for-duty program requires that individuals licensed to operate a nuclear reactor[60] meet several performance objectives, including "reasonable assurance" that they

- "are trustworthy and reliable as demonstrated by the avoidance of substance abuse," and
- "are not under the influence of any substance, legal or illegal, or mentally or physically impaired from

any cause, which in any way adversely affects their ability to safely and competently perform their duties."[61]

These programs also include "reasonable measures for the early detection of individuals who are not fit to perform the duties."[62] The regulations include training requirements[63] and penalties for violations,[64] as well as robust substance-abuse testing protocols.[65] The NRC also regulates access to national security information[66] and nuclear-related restricted data[67] by individuals working for entities regulated by the commission.[68]

The defense sector also tightly circumscribes processes on personnel clearances and the handling of sensitive classified information. For example, the National Industrial Security Program Operating Manual (Department of Defense guidance on the regulation of contractors in the industrial security sector) addresses contractors' protection of such information and the processes for contractor personnel to obtain clearances.[69]

Failure to have robust and adequate personnel safeguards can lead to significant harm inflicted by those on the inside. The Swiss financial institution UBS provides a telling example. A systems administrator who worked for UBS in New Jersey, Robert Duronio, wreaked havoc on company systems after reportedly expressing dissatisfaction with his salary and bonuses. Duronio planted a "logic bomb" in UBS's systems that activated after his departure and brought down roughly 2,000 UBS computers. The attack cost the company more than $3 million in repairs, in addition to lost revenue stemming from crippled trading capability.[70] (Duronio was sentenced to 97 months in prison.)[71]

We should assume that determined foreign adversaries are capable of hiring programmers who can damage American elections. We have certainly seen foreign governments engage in similar actions against private companies. In 2006, Dongfan "Greg" Chung, a former engineer at Boeing, was arrested for hoarding trade secrets about the U.S. space shuttle program with the intent to pass this information to the Chinese government. Federal agents found sensitive documents in his home, along with journals detailing his communications with Chinese officials. Chung was convicted in 2009 of economic espionage and acting as an agent of China,[72] and sentenced to 15 years in prison.[73]

TRANSPARENT OWNERSHIP

Lack of transparency into ownership and control of election vendors can mask foreign influence over an election vendor and corruption in local certification and contracting. We recommend mandated disclosure of significant — more than 5 percent — ownership interests and a prohibition on significant foreign ownership or control (with the option to request a waiver, if certain conditions are met). The purpose is not only to deter malfeasance and corruption but also to reassure voters that the motives of election vendors are aligned with the public's interest in free and fair elections.

The threats posed by foreign influence over a U.S. election vendor — including the heightened potential for foreign infiltration of the vendor's supply chain or knowledge of client election officials' capabilities and systems — should be obvious. A federal framework for securing elections should limit significant foreign ownership of election system vendors.

Over the last several years, the topic of foreign ownership of election vendors has occasionally made headlines.[74] In 2018, the FBI informed Maryland officials that a vendor servicing the state, ByteGrid LLC, had been under the control of a Russian oligarch with close ties to President Vladimir Putin.[75] In 2019, ByteGrid sold all of its facilities and customer agreements to a company called Lincoln Rackhouse.[76]

At the same time, lack of insight into election vendor ownership presents a serious risk that vendor-led influence campaigns and public officials' conflicts of interest will escape public scrutiny. Officials might award vendor contracts in exchange for gifts or special treatment rather than to those that would best facilitate free and fair elections. Transparency into ownership and control is required for the public to assess whether officials engaged in procurement and regulation have been improperly influenced.

There are a range of approaches to these problems of improper foreign and domestic influence. We recommend a stringent yet flexible standard: a requirement to disclose all entities or persons with a greater than 5 percent ownership or control interest, along with a ban on foreign ownership in that same amount,[77] with an option for the EAC to grant a waiver after consultation with DHS. While this proposal would address instances of foreign control over election vendors, such as ByteGrid, it could also impact companies such as Dominion Voting Systems, the second-largest voting machine vendor in the United States, whose voting machines are used by more than one-third of American voters and whose headquarters are in Toronto. Similarly, Scytl Secure Electronic Voting, which offers election night reporting and other election technologies to hundreds of election jurisdictions around the United States, is based in Barcelona.[78] A waiver would provide a means for these and other vendors with foreign ties to disclose those relationships and put in place safeguards to prevent foreign influence and alleviate security concerns, thus offering a reasonable path for a wide range of vendors to participate in the election technology market. Beyond this initial disclosure requirement, vendors should have an ongoing obligation to notify their customers and the EAC of any subsequent changes in their ownership or control.

The EAC can look to other sectors for examples of vendor disclosure of ownership or control agreements.

The Department of Defense's National Industrial Security Program Operating Manual is instructive. It requires companies to "complete a Certificate Pertaining to Foreign Interests when . . . significant changes occur to information previously submitted,"[79] and it requires vendors to submit reports when there is "any material change concerning the information previously reported by the contractor concerning foreign ownership control or influence."[80]

Lawmakers have already introduced legislation to improve transparency in ownership or control of election system vendors, with mechanisms ranging from disclosure requirements to strict bans on foreign ownership or control. One approach recently adopted in North Carolina requires disclosure of all owners with a stake of 5 percent or more in a vendor's company, subsidiary, or parent, so that the state's Board of Elections can consider this information before certifying a voting system.[81]

On the other end of the spectrum, the For the People Act and the SAFE Act would require that vendors in states receiving federal grants be owned and controlled by U.S. citizens or permanent residents, with no option for a waiver.[82] Similarly, the Election Vendor Security Act would have required each vendor to certify that "it is owned and controlled by a citizen, national, or permanent resident of the United States, and that none of its activities are directed, supervised, controlled, subsidized, or financed, and none of its policies are determined by, any foreign principal" or agent.[83]

Other proposals would prohibit foreign control but provide for a waiver, as we suggest. For instance, the Protect Election Systems from Foreign Control Act would require vendors to be "solely owned and controlled by a citizen or citizens of the United States" absent a waiver.[84] Such waivers could be granted if the vendor "has implemented a foreign ownership, control, or influence mitigation plan that has been approved by the [DHS] Secretary . . . ensur[ing] that the parent company cannot control, influence, or direct the subsidiary in any manner that would compromise or influence, or give the appearance of compromising or influencing, the independence and integrity of an election."[85]

With respect to defining an ownership or control interest of greater than 5 percent, the EAC could borrow from the approach used by the Federal Communications Commission (FCC). The FCC typically defines foreign ownership, including indirect ownership, by multiplying the percentage of shares an owner has in one company by the percentage of shares that company owns in a regulated broadcast or common carrier licensee. For instance, if a foreign person owned 30 percent of company A, and company A owned 25 percent of company B, the foreign person would be deemed to own 7.5 percent of company B. For purposes of voting shares, the FCC treats a majority stake as 100 percent, whereas for equity shares, the actual percentages are used.[86]

PROCESSES FOR REPORTING CYBER INCIDENTS

Both the public and local and state governments are often kept in the dark about security breaches that affect election vendors. This state of affairs can undermine faith in the vote and leave election officials unsure about vendor vulnerabilities. To address these concerns, vendors should face robust incident reporting requirements and a mandate to work with affected election authorities.

Federal oversight should require vendors to agree to report security incidents as a condition of certification. The Election Assistance Commission should require that vendors report to it and to all potentially impacted jurisdictions within days of discovering an incident. The EAC's existing Quality Monitoring Program requires only that vendors with certified voting equipment "submit reports of any voting system irregularities."[87] At present, the reporting requirement extends only to vendors of voting systems and does not encompass any other facets of those vendors' services, equipment, or operations. Election officials have long complained that vendors do not always share reports of problems with their systems.[88] Compounding the problem, a single vendor often serves many jurisdictions.[89]

Both the public and local and state governments are often **kept in the dark** about security breaches.

Some legislation has already sought to mandate more fulsome incident reporting by vendors. The Secure Elections Act, which had bipartisan support before losing momentum in 2018, included a mandatory reporting provision. Under the bill, if a so-called election service provider has "reason to believe that an election cybersecurity incident may have occurred, or that an information security incident related to the role of the provider as an election service provider may have occurred," then it must "notify the relevant election agencies in the most expedient time possible and without unreasonable delay (in no event longer than 3 calendar days after discovery of the possible incident)" and "cooperate with the election agencies in providing [their own required notifications]."[90]

Absent robust incident reporting, election officials and the public can be left unaware of potential threats that vendors might introduce into elections. As previously discussed, there is still considerable uncertainty concerning the alleged spearphishing attack and hack of a vendor involved in the 2016 elections. Much of what is known stems from the leak of a classified intelligence report obtained by the *Intercept,*[91] which identified the hacking victim as a Florida-based vendor, coupled with Special Counsel Robert Mueller's report to the attorney

general and indictment of 12 Russian intelligence officers.[92] Further complicating the picture of what happened, the Florida-based vendor, VR Systems, responded to an inquiry from Sen. Ron Wyden (D–OR) via letter, claiming that "based on our internal review, a private sector cyber security expert forensic review, and the DHS review, we are confident that there was never an intrusion in our EViD servers or network."[93] This uncertainty offers little for the vendor's clients to rely on in assessing the vendor's ongoing cyber readiness and whether to continue to contract with the vendor in future elections.

With mandated incident reporting, the EAC could provide the necessary assurance to election officials regarding the security of vendors by sharing information with election officials who need it, as well as by requiring appropriate remedial action, up to and including decertification.

SUPPLY CHAIN INTEGRITY

Federal regulators should require vendors to follow best practices for managing supply chain risks to election security. The new Technical Guidelines and Development Committee should define categories of subcontractors or products that pose serious risks, such as servers and server hosting, software development, transportation of sensitive equipment such as voting machines, and information storage. For instance, Liberty Systems, one of Unisyn Voting Solutions' regional partners, would likely be covered, given that it "provides election and vital statistics, software, and support throughout counties in the State of Illinois."[94] The TGDC's guidelines could then require that vendors have a framework to ensure that high-risk subcontractors and manufacturers also follow best practices on cybersecurity, background checks, and foreign ownership and control, as well as reporting cyber incidents to the vendor.

This approach is being used in other areas of government, where a growing recognition of supply chain risk to national security exists. The Department of Defense has recently stepped up its enforcement of supply chain integrity and security standards, requiring review of prime contractors' purchasing systems to ensure that Department of Defense contractual requirements pertaining to covered defense information and cyber incident reporting "flow down appropriately to . . . Tier 1 level suppliers" and that prime contractors have procedures in place for assessing suppliers' compliance with those requirements.[95]

The Department of Defense now requires that contractors handling controlled unclassified information (CUI) "flow down" contractual clauses to subcontractors whose "performance will [also] involve [the department's] CUI." The TGDC should develop an analogous category of subcontractors and manufacturers for which the same cybersecurity, background check requirements, and foreign ownership concerns that apply to election vendors would apply, based on the subcontractor's role and the opportunity for election security risk to be introduced.

Monitoring Vendor Compliance

To make its oversight most effective, the Election Assistance Commission must have the ability to confirm that federally certified vendors continue to meet their obligations. The fact that a vendor was, at some point in time, certified as meeting relevant federal standards is no guarantee that circumstances have not changed. Failure to stay in compliance should lead to appropriate remedial action by the EAC, up to and including decertification.

The EAC's Quality Monitoring Program for voting systems provides a starting point for how this might work. The EAC offers a mechanism for election officials on the ground to provide information about any voting system anomalies present in certified voting machines. If an election worker submits a credible report of an anomaly, the EAC distributes it to state and local election jurisdictions with similar systems, the manufacturer of the voting system, and the testing lab that certified the voting system.[96] According to the EAC's certification manual, "the Quality Monitoring Program is not designed to be punitive but to be focused on improving the process."[97] The program, then, is focused more on compliance than certification or decertification, although decertification can result in cases of persistent noncompliance.

The SAFE Act and the For the People Act call for the testing of voting systems nine months before each federal general election, as well as for the decertification of systems that do not meet current standards.[98]

A critical difference between the ability to monitor voting equipment and the practices of an election system vendor is that thousands of election officials and poll workers, and hundreds of millions of voters, interact with voting equipment on a regular basis. They can report anomalies when they see them. By contrast, most of the work of election system vendors happens out of public view.

For this reason, vendors must be obligated on an ongoing basis to remedy known security flaws or risk losing federal certification. Congress should provide the EAC with a mandate to ensure that vendors contract with independent security firms to conduct regular audits, penetration testing, and physical inspections and site visits, and to provide the results of those assessments to the EAC. One legislative proposal — the Protect Election Systems from Foreign Control Act — sought to do something similar by subjecting vendors to an annual evaluation to assess compliance with cybersecurity best practices.[99] The EAC's effectiveness in its new oversight role would be diminished absent some power to monitor vendors' efforts on this front — a power Congress ought to provide.

The EAC could require regular penetration testing by third parties to assess vendors' cyber readiness in real time. Such testing would give the EAC (and vendors) an opportunity to identify and remediate security flaws, hopefully before adversaries take advantage of them. The EAC should also consider using bug bounty programs, which have become a common tool deployed by private industry and government entities, including the Department of Defense.[100] Under bug bounty programs, friendly so-called white-hat hackers earn compensation for reporting vulnerabilities and risks to program sponsors. The For the People Act calls for such a program,[101] as does the Department of Justice's Framework for a Vulnerability Disclosure Program for Online Systems.[102]

Certified vendors should be required to submit to extensive inspection of their facilities. To assess compliance with cybersecurity best practices, personnel policies, incident reporting and physical security requirements, and the like, the EAC must be granted wide latitude to demand independent auditors' access to vendor systems and facilities. This should include unannounced, random inspections of vendors. The element of surprise could serve as a powerful motivator for vendors to stay in compliance with EAC guidance.

The Defense Contract Management Agency (DCMA) performs an analogous, if broader, role for military contractors. Serving as the Defense Department's "information brokers and in-plant representatives for military, Federal, and allied government buying agencies," DCMA's duties extend to both "the initial stages of the acquisition cycle and throughout the life of the resulting contracts."[103] In that latter stage of a contract, DCMA monitors "contractors' performance and management systems to ensure that cost, product performance, and delivery schedules are in compliance with the terms and conditions of the contracts."[104] This function includes having personnel in contractor facilities assess performance and compliance.[105] Although our proposal does not envision the EAC performing an ongoing contract compliance role, the EAC's enhanced oversight role could take some cues from DCMA's inspection protocols and ability to closely scrutinize vendors.

The NRC similarly holds inspection rights over those subject to its regulations, including companies that handle nuclear material and those holding licenses to operate power plants.[106] The NRC regulation requiring that those regulated "afford to the Commission at all reasonable times opportunity to inspect materials, activities, facilities, premises, and records under the regulations in this chapter" is of particular relevance to potential EAC oversight.[107] The NRC also has an extensive set of regulations concerning physical security at nuclear sites and of nuclear material.[108] Although these requirements are probably more onerous than those needed in the election sector (especially since nuclear material poses unique physical security risks), they could nonetheless prove instructive in crafting physical security requirements for vendors. Such requirements should go hand in hand with the cybersecurity best practices discussed above.

Enforcing Guidelines

It is critical to have a clear protocol for addressing election system vendor violations of federal guidelines. If states require their election offices to use only federally certified vendors, revocation of federal certification could have a potentially devastating impact on the ability of jurisdictions to run elections and ensure that every voter is able to cast a ballot.

Again, the Election Assistance Commission's process for addressing anomalies in voting equipment through its Quality Monitoring Program is instructive. If it finds that a system is no longer in compliance with the VVSG, the manufacturer is sent a notice of noncompliance. This is not a decertification of the machine but rather a notification to the manufacturer of its noncompliance and its procedural rights before decertification. The manufacturer has the right to present information, access the information that will serve as the basis of the decertification decision, and cure system defects prior to decertification. The right to cure system defects is limited; it must be done before any individual jurisdiction that uses the system next holds a federal election.[109]

If decertification moves forward after attempts to cure or opportunities to submit additional information, the manufacturer may appeal the decision. If the appeal is denied, then the decertified voting system will be treated as any other uncertified system. The EAC will also notify state and local election officials of the decertification.[110] A decertified system may be resubmitted for certification and will be treated as any other system seeking certification.

The EAC's application of this process to the ES&S voting system Unity 3.2.0.0 provides an example of how this can happen. Certification of this system was granted in 2009.[111] In 2011, the EAC's Quality Monitoring Program received information about an anomaly in the system and began a formal investigation.[112] A notice of noncompliance was then sent to ES&S in 2012, listing the specific anomalies found in the voting system and informing ES&S that if these anomalies were not remedied, the EAC would be obligated to decertify the voting system.[113] ES&S attempted to cure the defects, as was its right, and produced a new, certified version of the Unity system.[114] The vendor then requested that its old system be withdrawn from the list of EAC certified systems.[115]

Decertification of a vendor would need to be handled thoughtfully, so that local election officials are not left scrambling to contract new election services close to an election. In this sense, close coordination among federal and local officials and relevant vendors to proactively identify and fix issues would be necessary for any scheme

to succeed. The EAC would also have to be left with the flexibility to decide what, if any, equipment and services could no longer be used or sold as federally certified. To that end, decertification should incorporate these key elements:

- A voting system decertification should not necessarily result in a vendor decertification and vice versa. For instance, a voting machine vendor might be found to be out of compliance with federal requirements for background checks on employees. If the EAC determines this noncompliance did not impact the security of voting machines already in the field, it could leave the voting system certified but ban the vendor from selling additional machines (or certain employees from servicing existing machines) until the failure is remedied. Alternatively, it could allow the vendor's voting machines to continue to be used for a limited time, subject to additional security measures, such as extra preelection testing and postelection audits.
- There should be a clear process ahead of a formal decertification, with notification to affected state and local officials and plenty of opportunities for the relevant vendor to address issues before the EAC takes more drastic action. Only the most urgent and grave cybersecurity lapses should truncate this decertification process.
- Any decertification order should include specific guidance to state and local officials on how existing vendor products or services are affected, assistance to those officials with replacing those goods or services (if necessary), and a road map for the vendor to regain certification.

Conclusion

Private election vendors play a crucial role in securing the nation's elections against malicious actors who have already taken steps toward compromising elections and the public's confidence in our democracy. Yet these vendors are currently subject to little oversight to ensure that they remain secure against these threats and that many of the products and services they provide, such as electronic pollbooks, are secure. Currently, only voting systems — the systems used to cast and tabulate ballots — are subject to robust federal oversight, and then only via a voluntary certification program. We recommend that Congress empower the Election Assistance Commission to certify election vendors more broadly as compliant with voluntary guidelines relating to cybersecurity, personnel, transparent ownership and control, reporting of cyber incidents, and supply chain integrity. In the meantime, the EAC should employ its registration and certification processes to ensure that vendors of certified voting systems keep up with these practices.

Endnotes

1 Kim Zetter, "The Crisis of Election Security," *New York Times Magazine*, Sept. 26, 2018, https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html.

2 The For the People Act, H.R. 1, 116th Cong. (2019) and the Securing America's Federal Elections Act, the SAFE Act, H.R. 2722, 116th Cong. (2019) both would accomplish much, but not all, of this report's recommendations. Specifically, these bills provide for EAC oversight of a broader array of election system products and vendors in exchange for receipt and use of federal funds but do not provide for ongoing certification and monitoring of vendors. They also do not speak to best practices on personnel decisions or supply chain security. These bills also do not fully address how to define foreign ownership and control. Where this report's recommendations could be accomplished by adopting one of these bills, we have attempted to flag that for the reader.

3 Compare, for example, The Labeling of Hazardous Art Materials Act, 15 U.S.C. 1277, and 16 C.F.R. §§ 1500.14, with 11 CFR §§ 9405.1 et seq. Indeed, Chapter II of Title 11 of the Code of Federal Regulations, the principal regulations applicable to the EAC, does not address the certification of voting systems or any potential oversight of election vendors more broadly. Nor does the legislation that established the EAC (the Help America Vote Act of 2002) — which sets some requirements for voting systems used in federal elections, see 52 U.S.C. § 21081 — require the EAC to issue any mandatory regulations on those topics. See, e.g., 52 U.S.C § 20971 (regarding the certification and testing of voting systems), § 20929 ("The Commission shall not have any authority to issue any rule, promulgate any regulation, or take any other action which imposes any requirement on any State or unit of local government . . ."), § 21101 (regarding the EAC's adoption of *voluntary* guidance).

4 *Hearing on Election Security, Before the Comm. on House Administration*, 116th Cong. (May 8, 2019) (statement of Zoe Lofgren, chairperson).

5 *Hearing on Election Security, Before the Comm. on House Administration*, 116th Cong. (May 8, 2019) (statement of John Merrill, Alabama secretary of state).

6 U.S. Senate Select Committee on Intelligence, *Report of the Select Committee on Intelligence, U.S. Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1*, July 5, 2019, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf ("State election officials, who have primacy in running elections, were not sufficiently warned or prepared to handle an attack from a hostile nation-state actor."); U.S. Const. art. I, § 4 (permitting Congress to regulate elections); U.S. Const. art. IV, § 4 (requiring Congress to guarantee a republican form of government to the states and to protect them from invasion).

7 Lorin Hitt et al., *The Business of Voting: Market Structure and Innovation in the Election Technology Industry*, University of Pennsylvania Wharton School, 2017, 15, https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

8 Frank Bajak, "US Election Integrity Depends on Security-Challenged Firms," Associated Press, Oct. 29, 2018, https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c (quoting Sen. Ron Wyden).

9 Hitt et al., *The Business of Voting*, 7.

10 Hitt et al., *The Business of Voting*, 8.

11 U.S. Senate Select Committee on Intelligence, *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations,* May 8, 2018, https://www.intelligence.senate.gov/publications/russia-inquiry.

12 United States v. Netyksho et al., No. 1:18CR00215, 2018 WL 3407381, 26 (D.D.C. Jul. 13, 2018); Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election, U.S. Department of Justice, 2019, 50,* https://www.justice.gov/storage/report.pdf; Casey Tolan, "Humboldt County Shores Up Voting Systems after Russian Hack of Election Contractor," *Mercury News,* June 6, 2017, https://www.mercurynews.com/2017/06/06/humboldt-county-moves-to-shore-up-voting-systems-after-election-contractor-hack (listing VR Systems' own website as the source for its list of states in which the company operates).

13 Sam Biddle, "A Swing-State Election Vendor Repeatedly Denied Being Hacked by Russians. The New Mueller Indictment Says Otherwise," *Intercept,* July 13, 2018, https://theintercept.com/2018/07/13/a-swing-state-election-vendor-repeatedly-denied-being-hacked-by-russians-new-mueller-indictment-says-otherwise.

14 United States v. Netyksho et al., No. 1:18CR00215, 2018 WL 3407381, 26 (D.D.C. Jul. 13, 2018).

15 Miles Parks, "Florida Governor Says Russian Hackers Breached Two Counties in 2016," NPR, May 14, 2019, https://www.npr.org/2019/05/14/723215498/florida-governor-says-russian-hackers-breached-two-florida-counties-in-2016.

16 Kim Zetter, "Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials," *Vice,* Aug. 8, 2019, https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials (quoting ES&S marketing literature).

17 Dan O'Sullivan, "The Chicago Way: An Electronic Voting Firm Exposes 1.8M Chicagoans," *Upguard*, Dec. 13, 2018, https://www.upguard.com/breaches/cloud-leak-chicago-voters.

18 Bajak, "US Election Integrity."

19 "Report Blames Software Error for Los Angeles Voting Problem," Associated Press, Aug. 1, 2018, https://www.apnews.com/95b056ab2eab47febaf721a1d285a045; IBM Security Services, *Independent Investigation of Election System Anomalies in Los Angeles County on June 5, 2018,* Aug. 1, 2018, http://file.lacounty.gov/SDSInter/lac/1042885_FINALExecutiveSummaryAugust12018.pdf; See also Board of Supervisors, *Request for Approval: Amendment Number Eight to Agreement Number 76010 with Data Information Management Systems, LLC for Voter Information Management System Maintenance and Support Services*, County of Los Angeles, 2015, https://www.lavote.net/documents/05052015.pdf (identifying ES&S subsidiary Data Information Management Systems, LLC, as vendor responsible for maintaining and servicing Los Angeles County's voter information management system).

20 U.S. Election Assistance Commission, "Quality Monitoring Program," https://www.eac.gov/voting-equipment/quality-monitring-program.

21 National Protection and Programs Directorate, "DHS and Private Sector Partners Establish Information and Communications Technology Supply Chain Risk Management Task Force," U.S. Department of Homeland Security, Oct. 30, 2018, https://www.dhs.gov/news/2018/10/30/dhs-and-private-sector-partners-establish-information-and-communications-technology.

22 See, e.g., Sean Keane, "Huawei Ban: Full Timeline on How and Why Its Phones Are Under Fire," *CNET*, May 30, 2019, https://www.cnet.com/news/huawei-ban-full-timeline-on-how-and-why-its-phones-are-under-fire.

23 Unisyn Voting Systems, "Partners," https://unisynvoting.com/partners.

24 The EAC's bipartisan structure provides important checks and balances, but it also carries a risk of the sort of pervasive gridlock that has hamstrung the Federal Election Commission, leading the Brennan Center to advocate for a fundamental overhaul of that agency. See Daniel I. Weiner, *Fixing the FEC: An Agenda for Reform, Brennan Center for Justice*, 2019, https://www.brennancenter.org/sites/default/files/publications/2019_04_FECV_Final.pdf. But the EAC's mission is very different from that of the FEC, which oversees campaign finance.

Because of the technical nature of much of its work, the EAC has not been paralyzed by the same partisan ideological divisions, leading us to conclude that its bipartisan structure remains viable, at least for now.

25 Ian Urbina, "Panel Said to Alter Finding on Voter Fraud," *New York Times,* Apr. 11, 2007, https://www.nytimes.com/2007/04/11/washington/11voters.html.

26 Eric Geller, "Federal Election Official Accused of Undermining His Own Agency," *Politico,* June 15, 2019, https://www.politico.com/story/2019/06/15/federal-election-brian-newby-2020-1365841.

27 Kim Zetter, "Experts: Elections Commission Downplaying Unseen Risks to 2020 Vote," *Politico,* Mar. 15, 2019, https://www.politico.com/story/2019/03/15/election-machine-security-2020-cybersecurity-1222803.

28 Geller, "Federal Election Leader Accused."

29 U.S. Election Assistance Commission, *Fiscal Year 2019 Congressional Budget Justification,* Feb. 12, 2018, https://Www.Eac.Gov/Assets/1/6/Fy_2019_Cbj_Feb_12_2018_Final.Pdf; Omnibus Appropriations Act, 2009, Pub. L. No. 111-8 (2009); Election Assistance Commission Termination Act, H.R. Rept. 114-361 (2015).

30 Both the House and Senate held EAC oversight hearings this year, but they were the first oversight hearings in either chamber in over eight years. See Committee on House Administration, "Hearings," https://cha.house.gov/committee-activity/hearings; "Congressional Hearings," Govinfo, https://www.govinfo.gov/app/collection/chrg/116/house/Committee%20on%20House%20Administration; Senate Committee on Rules and Administration, "Hearings," https://www.rules.senate.gov/hearings.

31 Under the Help America Vote Act, Pub. L. No. 107-252 (2002), this includes all equipment that is used to "define ballots; . . . cast and count votes; . . . report or display election results; and . . . maintain and product any audit trail information." It does not include certification of other election systems, such as electronic pollbooks; such machines are now used widely and are critical to running elections around the country. See Andrea Cordova, "Want a Simple Way to Increase Election Security? Use Paper," Brennan Center for Justice, Oct. 8, 2018, https://www.brennancenter.org/blog/want-simple-way-increase-election-security-use-paper. They, too, should be added to this system testing regime, as was proposed recently in the Election Security Assistance Act, H.R. 3412, 116th Cong. (2019), § 3(a) .

32 The EAC can conduct manufacturing site visits through its Quality Monitoring Program, but a site visit is unlikely to uncover insecure development practices, which can pose problems at later stages, such as during the provision of technical support to election officials or the programming of a ballot style or candidate register.

33 For the People Act, H.R. 1, 116th Cong. (2019), § 3302; Securing America's Federal Elections Act, H.R. 2722, 116th Cong. (2019), § 204; Election Security Assistance Act, H.R. 3412, 116th Cong. (2019), § 3(a).

34 U.S. Election Assistance Commission, *Voluntary Voting System Guidelines,* Vol. 1, Version 1.1, 2015, https://www.eac.gov/assets/1/28/VVSG.1.1.VOL.1.FINAL1.pdf.

35 U.S. Election Assistance Commission, *VVSG Public Hearing (Apr. 10, 2019)* (statement of Vice Chairman Ben Hovland).

36 U.S. Election Assistance Commission, *Testing and Certification Program Manual, Version 2.0, 2015, 71,* https://www.eac.gov/assets/1/6/Cert_Manual_7_8_15_FINAL.pdf.

37 *Testing and Certification Program Manual, Version 2.0, EAC, 71-75.*

38 Election Vendor Security Act, H.R.6435, 115th Cong. (2018).

39 For the People Act, H.R. 1, 116th Cong. (2019), § 298A; Securing America's Federal Elections Act, H.R. 2722, 116th Cong. (2019), § 297A.

40 U.S. Election Assistance Commission, "Fact Sheet: The U.S. Election Assistance Commission's Voting System Testing and Certification Program," Mar. 7, 2017, https://www.eac.gov/news/2017/03/07/fact-sheet-the-us-election-assistance-commissions-voting-system-testing-and-certification-program-voting-systems-certification-communications-fact-sheet.

41 U.S. Department of Homeland Security, *Election Infrastructure Subsector Coordinating Council Charter,* Version 1.0, 2018, 3, https://www.dhs.gov/sites/default/files/publications/govt-facilities%20-EIS-scc-charter-2018-508.pdf.

42 When the TGDC advised a restructuring of the VVSG in 2007, its recommendations were never adopted. Work began on a "patch," the VVSG 1.1, but that was halted for years, when the EAC lost a quorum, and was ultimately adopted only in 2015. A new VVSG 2.0 was provided by the TGDC in Feb. 2017 and was recommended for adoption that September, but again the EAC lost its quorum. It is now out for public comment. U.S Election Assistance Commission, VVSG Public Hearing Apr. 10, 2019) (statement of Ryan Macias), https://www.eac.gov/events/2019/04/10/vvsg-public-hearing.

43 U.S. Election Assistance Committee, "Technical Guidelines Development Committee," https://www.eac.gov/about/technical-guidelines-development-committee/.

44 Voting System Cybersecurity Act of 2019, S. 1454, 116th Cong. (2019), § 2.

45 A possible configuration of the NIST-chosen representatives could be

- one representative from CISA with technical and scientific expertise related to cybersecurity in election technology;
- one representative of state election information technology directors selected by the National Association of State Election Directors;
- one representative from the National Association of State Chief Information officers (NACIO) with expertise in cybersecurity;
- one representative from the EI-ISAC with technical and scientific expertise related to cybersecurity in elections;
- two representatives who are academic or scientific researchers with technical and scientific expertise related to cybersecurity, chosen by NIST;
- one representative who possesses technical and scientific expertise relating to the accessibility and usability of voting systems, chosen by NIST;
- one representative of manufacturers of voting system hardware and software who possesses technical and scientific expertise relating to cybersecurity and the administration of elections, selected jointly by the EAC and NIST; and
- one representative of a laboratory accredited under section 231(b) who possesses technical and scientific expertise relating to cybersecurity and the administration of elections, selected by the NIST National Voluntary Laboratory Assessment Program (NVLAP).

A similar proposal to modify the TGDC appears in S. Amdt. 3983 to H.R. 6157, 115th Cong. (2018).

46 Currently, guidelines issued by the TGDC do not go into effect absent approval by the EAC, which can create significant delays, and voting system vendors have obtained certification to older versions of the VVSG, even after new versions have been approved by the EAC. See Tim Starks, "EAC Finally Nearing Ability to Take Major Action," *Politico*, Nov. 28, 2018, https://www.politico.com/newsletters/morning-cybersecurity/2018/11/28/eac-finally-nearing-ability-to-take-major-action-433181 (describing the EAC's lack of a quorum since March 2018, which prevented it from approving a new version of the VVSG). See U.S. Election Assistance Commission, "Certified Voting Systems," https://www.eac.gov/voting-equipment/certified-voting-systems (showing voting systems as certified in 2017, 2018, and 2019 to VVSG 1.0, a set of guidelines that was replaced by VVSG 1.1 in 2015).

47 Philip Bump, "Timeline: How Russian Agents Allegedly Hacked the DNC and Clinton's Campaign," *Washington Post*, July 13, 2018, https://www.washingtonpost.com/news/politics/wp/2018/07/13/timeline-how-russian-agents-allegedly-hacked-the-dnc-and-clintons-campaign/?utm_term=.618a5496022b; Eric Lipton, David E. Sanger, and Scott Shane, "The Perfect Weapon: How Russian Cyberpower Invaded the U.S.," *New York Times,* Dec. 13, 2016, https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

48 Lipton et al., "The Perfect Weapon."

49 Lipton et al., "The Perfect Weapon."

50 Eric Geller, "Microsoft Reveals First Known Midterm Campaign Hacking Attempts," *Politico,* July 19, 2018, https://www.politico.com/story/2018/07/19/midterm-campaign-hacking-microsoft-733256; Kevin Poulsen and Andrew Desiderio, "Russian Hackers' New Target: A Vulnerable Democratic Senator," *Daily Beast,* July 26, 2018, https://www.thedailybeast.com/russian-hackers-new-target-a-vulnerable-democratic-senator; Andy Kroll, "Documents Reveal Successful Cyberattack in California Congressional Race," *Rolling Stone,* Aug. 15, 2018, https://www.rollingstone.com/politics/politics-news/california-election-hacking-711202.

51 Using remote-access software to access a computer risks opening up access to the entire network that computer is connected to. Yet it has been alleged that VR systems used such software in 2016 to connect to the North Carolina State Board of Elections, in order to download a voter list for Durham County. Kim Zetter, "Software Vendor May Have Opened a Gap for Hackers in 2016 Swing State," *Politico*, June 5, 2019, https://www.politico.com/story/2019/06/05/vr-systems-russian-hackers-2016-1505582.

52 Mueller, *Report on the Investigation into Russian Interference*, 51; Kim Zetter, "Florida Election Vendor Says It Has Proof It Wasn't Breached by Russians," *Politico,* May 23, 2019, https://www.politico.com/story/2019/05/23/florida-vendor-russia-1469086.

53 Securing America's Federal Elections Act, H.R. 2722, 116th Cong. (2019), § 297A; Election Security Act, H.R. 2660, 116th Cong. (2019), § 297A; Election Security Act of 2019, S. 1540, 116th Cong. (2019), § 297A; For the People Act, H.R. 1, 116th Cong. (2019), § 298A.

54 National Institute of Standards and Technology, "Cybersecurity Framework," https://www.nist.gov/cyberframework.

55 National Institute of Standards and Technology, "Questions & Answers," https://www.nist.gov/cyberframework/questions-and-answers#checklist.

56 Patricia Toth, *NIST Handbook 162: NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements*, National Institute for Standards and Technology, 2017, https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf. See also, "DFARS Cybersecurity Requirements," Manufacturing Extension Partnership, National Institute of Standards and Technology, created Dec. 1, 2017, updated June 28, 2018, https://www.nist.gov/mep/cybersecurity-resources-manufacturers/dfars800-171-compliance.

57 U.S. Department of Homeland Security, "Cyber Resilience Review," https://www.us-cert.gov/sites/default/files/c3vp/crr-fact-sheet.pdf.

58 See generally U.S. Department of Homeland Security, "Cybersecurity Framework," Critical Infrastructure Cyber Community Voluntary Program, https://www.us-cert.gov/ccubedvp/cybersecurity-framework.

59 U.S. Nuclear Regulatory Commission, "About NRC," last updated Feb. 12, 2018, https://www.nrc.gov/about-nrc.html.

60 See generally, 10 C.F.R. §§ 26.1–26.825.

61 10 C.F.R. § 26.23.

62 10 C.F.R. § 26.23.

63 10 C.F.R. § 26.29.

64 10 C.F.R. §§ 26.181–26.189.

65 10 C.F.R. §§ 26.81–26.119.

66 10 C.F.R. § 10.5 ("*National Security Information* means information that has been determined under Executive Order 13526 or any predecessor or successor order to require protection against unauthorized disclosure and that is so designated.").

67 10 C.F.R. § 10.5 ("*Restricted Data* means all data concerning design, manufacture, or utilization of atomic weapons, the production of special nuclear material, or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 142 of the Atomic Energy Act of 1954, as amended.").

68 10 C.F.R. § 10.1(a) ("This part establishes the criteria, procedures, and methods for resolving questions concerning:…(3) The eligibility of individuals who are employed by or are applicants for employment with NRC licensees, certificate holders, holders of standard design approvals under part 52 of this chapter, applicants for licenses, certificates, and NRC approvals, and others who may require access related to a license, certificate, or NRC approval, or other activities as the Commission may determine, for access to Restricted Data under the Atomic Energy Act of 1954, as amended, and the Energy Reorganization Act of 1974, or for access to national security information.").

69 National Industrial Security Program, *Operation Manual, Feb. 2006*, §§ 2-200–2-211, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf.

70 U.S. Department of Justice, "Disgruntled UBS PaineWebber Employee Charged with Allegedly Unleashing 'Logic Bomb' on Company Computers," Dec. 17, 2002, https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/duronioIndict.htm; Stephen Foley, "Disgruntled Worker 'Tried to Cripple UBS in Protest over $32,000 Bonus'," *Independent,* June 8, 2006, https://www.independent.co.uk/news/business/news/disgruntled-worker-tried-to-cripple-ubs-in-protest-over-32000-bonus-481515.html.

71 Ericka Chickowski, "Former UBS System Administrator Gets Eight Years for Logic Bomb," *SC Media,* Dec. 18, 2006, https://www.scmagazineuk.com/article/1467247.

72 U.S. Department of Justice, "Former Boeing Engineer Convicted of Economic Espionage in Theft of Space Shuttle Secrets for China," July 16, 2009, https://www.justice.gov/opa/pr/former-boeing-engineer-convicted-economic-espionage-theft-space-shuttle-secrets-china.

73 "Chinese-Born Engineer Gets 15 Years for Spying," Associated Press, Feb. 8, 2010, http://www.nbcnews.com/id/35300466/ns/us_news-security/t/chinese-born-engineer-gets-years-spying/#.XUrYm-hKg2w.

74 For example, there were reports that Venezuelan interests with ties to the Venezuelan government owned the parent company of an election vendor, Sequoia Voting Systems, which Dominion later acquired. See Tim Golden, "U.S. Investigates Voting Machines' Venezuela Ties," *New York Times*, Oct. 29, 2006, https://www.nytimes.com/2006/10/29/washington/29ballot.html. The Venezuelan owners of Sequoia's parent company eventually agreed to sell Sequoia. See Zachary A. Goldfarb, "U.S. Drops Inquiry of Voting Machine Firm," *Washington Post,* Dec. 23, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/12/22/AR2006122201304.html.

75 Mark Morales, "Maryland Election Contractor Has Ties to Russian Oligarch," CNN, July 16, 2018, https://www.cnn.com/2018/07/16/politics/maryland-elections-russia/index.html; Chase Cook and E.B. Furgurson III, "FBI Informs Maryland of Election Software Owned by Russian Firm, No Known Breaches," *Capital Gazette,* July 13, 2018, https://www.capitalgazette.com/news/government/ac-cn-russian-election-0714-story.html.

76 Rich Miller, "Lincoln Rackhouse Continues Expansion With Purchase of ByteGrid," *Data Center Frontier,* May 8, 2019, https://datacenterfrontier.com/lincoln-rackhouse-continues-expansion-with-purchase-of-bytegrid.

77 We recommend defining "foreign national" as someone who is neither a U.S. citizen nor a U.S. permanent resident, as this is the definition used by the FEC in prohibiting foreign contributions to candidates.

78 Jordan Wilkie, "'They Think They Are Above the Law': The Firms that Own America's Voting System," *Guardian*, Apr. 23, 2019, https://www.theguardian.com/us-news/2019/apr/22/us-voting-machine-private-companies-voter-registration; Hitt et al., *The Business of Voting*; Scytl, "US Elections," https://www.scytl.com/en/customers/us-elections.

79 National Industrial Security Program, *Operation Manual*, Feb. 2006, § 2-302, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf.

80 National Industrial Security Program, *Operation Manual*, **§1-**

302(g)(5).

81 North Carolina Board of Elections, *Election Systems Certification Program,* amended June 2019, 3–20, https://s3.amazonaws.com/dl.ncsbe.gov/State_Board_Meeting_Docs/2019-06-13/Voting%20System%20Certification/NCSBEVotingSystemsCertificationProgram_06132019.pdf; Ben Popken, "State Officials Demand Voting System Vendors Reveal Owners after Russian Hacks and Investments," NBC News, June 24, 2019, https://www.nbcnews.com/politics/elections/voting-system-vendors-reveal-owners-after-russian-hacks-investments-n1020956.

82 For the People Act, H.R. 1, 116th Cong. (2019), § 298A; Securing America's Federal Elections Act, H.R. 2722, 116th Cong. (2019), § 297A.

83 Election Vendor Security Act, H.R. 6435, 115th Cong. (2018).

84 Protect Election Systems from Foreign Control Act, H.R. 6449, 115th Cong. (2018).

85 Protect Election Systems from Foreign Control Act, H.R. 6449, 115th Cong. (2018).

86 In Review of Foreign Ownership Policies for Broadcast, Common Carrier and Aeronautical Radio Licensees under Section 310(b)(4) of the Communications Act of 1934, as Amended, FCC 16-128, §1.5001(f) (Sept. 29, 2016).

87 U.S. Election Assistance Commission, "Frequently Asked Questions: Voting System Certification Questions," https://www.eac.gov/voting-equipment/frequently-asked-questions.

88 Lawrence Norden, *Voting System Failures: A Database Solution,* 2010, 9, https://www.brennancenter.org/sites/default/files/legacy/Democracy/Voting_Machine_Failures_Online.pdf.

89 Hitt et al., *The Business of Voting,* 9–27.

90 Secure Elections Act, S. 2261, 115th Cong. (2017); in a similar vein, the Election Vendor Security Act, H.R. 6435, 115th Cong. (2018), requires vendors to "report any known or suspected security incidents involving election systems . . . not later than 10 days after the vendor first knows or suspects that the incident occurred."

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

92 United States v. Netyksho et al., No. 1:18CR00215, 2018 WL 3407381, at 26 (D.D.C. Jul. 13, 2018).

93 VR Systems, Letter to Sen. Ron Wyden, May 16, 2019, https://www.politico.com/f/?id=0000016a-e72c-d72a-af6e-f72eb6550002. According to the letter, EViD "is a front-end system used to check voters in at the polls and to provide information such as a voter's polling location when they search for it."

94 Liberty Systems, LLC, "About Us," http://libertysystemsllc.com/.

95 Undersecretary of Defense, *Memorandum Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review, U.S. Department of Defense,* Jan. 21, 2019, https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA000140-19%20TAB%20A%20USD(AS)%20Signed%20Memo.pdf.

96 U.S. Election Assistance Commission, *Testing and Certification Program Manual, Version 2.0*, 71.

97 U.S. Election Assistance Commission, *Testing and Certification Program Manual, Version 2.0*, 73.

98 Securing America's Federal Elections Act, H.R. 2722, 116th Cong. (2019), § 202; For the People Act, H.R. 1, 116th Cong. (2019), § 3301.

99 Protect Election Systems from Foreign Control Act, H.R. 6449, 115th Cong. (2018), § 304.

100 U.S. Department of Defense, "Department of Defense Expands 'Hack the Pentagon' Crowdsourced Digital Defense Program," Oct. 24, 2018, https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr.

101 For the People Act, H.R. 1, 116th Cong. (2019), § 3402.

102 *A Framework for a Vulnerability Disclosure Program for Online Systems, Version 1.0,* Cybersecurity Unit, Computer Crime & Intellectual Property Section, Criminal Division, U.S. Department of Justice, July 2017, https://www.justice.gov/criminal-ccips/page/file/983996/download.

103 Defense Contract Management Agency, "About the Agency," https://www.dcma.mil/About-Us/.

104 Defense Contract Management Agency, "About the Agency."

105 See generally, Defense Contract Management Agency, "What DCMA Does," Aug. 22, 2016, https://www.dcma.mil/News/Videos/videoid/480264/nav/Default/.

106 10 C.F.R. §§ 19.1–19.40.

107 10 C.F.R. § 19.14(a).

108 10 C.F.R. §§ 73.1–73.81.

109 U.S. Election Assistance Commission, *Testing and Certification Program Manual, Version 2.0*, 65.

110 U.S. Election Assistance Commission, *Testing and Certification Program Manual, Version 2.0*, 69.

111 Thomas R. Wilkey (executive director, U.S. Election Assistance Commission), letter to Steve Pearson (vice president, Election Systems & Software), July 21, 2009, https://www.eac.gov/voting-equipment/-unity-3200.

112 Brian J. Hancock (director, Testing & Certification Program, U.S. Election Assistance Commission), letter to Steve Pearson (vice president, Election Systems & Software), Mar. 1, 2011, https://www.eac.gov/voting-equipment/-unity-3200.

113 Mark Robbins (general counsel and acting executive director, U.S. Election Assistance Commission), letter to Steve Pearson (vice president, Election Systems & Software), Feb. 1, 2012, https://www.eac.gov/voting-equipment/-unity-3200.

114 Steve Pearson (vice president, Election Systems & Software), letter to Mark Robbins (general counsel and acting executive director, U.S. Election Assistance Commission), Feb. 7, 2012, https://www.eac.gov/voting-equipment/-unity-3200.

115 Kathy Rogers (vice president, Election Systems & Software), letter to Brian J. Hancock (director, Testing & Certification Program, U.S. Election Assistance Commission), Aug. 3, 2012, https://www.eac.gov/voting-equipment/-unity-3200.

Endnotes for Sidebar

i U.S. Election Assistance Commission, *Testing and Certification Program Manual, Version 2.0,* 12–19.

ii *Voluntary Voting Systems Guidelines, Vol.1, Version 1.1,* §7.4.6, §7.5, §7.5.2, §7.5.3.

iii The adoption of modern approaches such as agile software development and the provision of ongoing technical support makes information about a vendor's ongoing compliance with best practices critical for determining the level of risk posed by upgrades and changes, including some that might be deemed de minimis if vendor security practices are strong. See U.S. Election Assistance Commission, *Testing and Certification Program Manual, Version 2.0*.

iv U.S. Election Assistance Commission, *Testing and Certification Program Manual, Version 2.0*, 17. Suspension of an entire vendor, like decertification of a vendor, would similarly need to be handled thoughtfully. See Enforcing Guidelines section on this report.

Image Credits:

Page 5: REVA/Noun Project, Pravin Unagar/Noun Project, Aisyah/

ABOUT THE AUTHORS

▶ **Lawrence Norden** is director of the Election Reform Program at the Brennan Center for Justice, where he leads efforts to bring balance to campaign funding and break down barriers that keep Americans from participating in politics, ensure that U.S. election infrastructure is secure and accessible to every voter, and protect elections from foreign interference. He has authored several nationally recognized reports and articles related to voting rights and voting technology, including *Securing Elections From Foreign Interference* (2017), *America's Voting Machines at Risk* (2015), and *How to Fix Long Lines* (2013). His work has been featured in media outlets across the country, including the *New York Times*, the *Wall Street Journal*, Fox News, CNN, MSNBC, and National Public Radio. He has testified before Congress and several state legislatures on numerous occasions. Norden is a member of the Election Assistance Commission's Board of Advisors. This report is not affiliated with his role as an EAC advisor. He is a graduate of the University of Chicago and NYU School of Law.

▶ **Christopher R. Deluzio** is the policy director of the University of Pittsburgh's Institute for Cyber Law, Policy, and Security. He was previously counsel in the Democracy Program at the Brennan Center for Justice, where his writing included nationally recognized work on voter purges, a procurement guide to assist in the selection and management of election vendors, and legal analysis of speech restrictions in polling places. Prior to joining the Brennan Center, he was a litigation associate in private practice with Wachtell, Lipton, Rosen & Katz and, before that, law clerk to Judge Richard J. Sullivan of the U.S. District Court for the Southern District of New York. He graduated magna cum laude from Georgetown Law, where he was elected to the Order of the Coif, served as an executive articles editor of the *Georgetown Law Journal*, and was selected as the top oralist in the Robert J. Beaudry Moot Court Competition and the Thurgood A. Marshall Memorial Moot Court Competition. He received a bachelor's degree from the U.S. Naval Academy and, following graduation, served as an active-duty naval officer.

▶ **Gowri Ramachandran** is senior counsel in the Brennan Center for Justice's Democracy Program. She comes to the Brennan Center from Southwestern Law School in Los Angeles, California, where she is on leave from her position as professor of law. At Southwestern, she taught courses in constitutional law, employment discrimination, and critical race theory, as well as the Ninth Circuit Appellate Litigation Clinic, which received the Ninth Circuit's 2018 Distinguished Pro Bono Service Award. She received her undergraduate degree in mathematics from Yale College and a master's degree in statistics and JD from Harvard University. While in law school, she served as editor in chief of the *Yale Law Journal*. After graduating from law school in 2003, Ramachandran served as law clerk to Judge Sidney R. Thomas of the U.S. Court of Appeals for the Ninth Circuit in Billings, Montana. After a fellowship at Georgetown Law, she joined the Southwestern faculty in 2006.

ACKNOWLEDGMENTS

The Brennan Center gratefully acknowledges BLT Charitable Trust, Carnegie Corporation of New York, Craig Newmark Philanthropies, Ford Foundation, Lee Halprin and Abby Rockefeller, The JPB Foundation, Leon Levy Foundation, Open Society Foundations, Barbara B. Simons, Wallace Global Fund, and Leslie Williams for their generous support of our election security work.

The authors would like to thank the numerous Brennan Center colleagues who collaborated in preparing this report. Brennan Center Fellow Derek Tisler and Legal Intern Cara Ortiz contributed crucial research and editorial support. Edgardo Cortés, Elizabeth Howard, and Daniel I. Weiner provided helpful revisions. Jeanne Park and Matthew Harwood of the Brennan Center's communications team lent valuable review and editing assistance. The authors are grateful to Research and Program Associate Andrea Córdova McCadney for assistance in citation-checking and editing. The editorial and design assistance of Alexandra Ringe, Alden Wallace, Rebecca Autrey, and Zachary Laub allowed this report to reach publication.

This report also benefited from the many people willing to share their valuable expertise and provide insight in the review process. We gratefully acknowledge the following individuals for their helpful feedback: Marian Schneider, president, Verified Voting; Ryan Macias, election technology and security expert; Susan Greenhalgh, vice president for programs, National Election Defense Coalition; Bruce Schneier, security technologist and adjunct lecturer in public policy, Harvard Kennedy School; Gregory A. Miller, cofounder and chief operating officer, OSET Institute; E. John Sebes, cofounder and chief technology officer, OSET Institute; and Eddie Perez, global director of technology R&D, OSET Institute.

BRENNAN CENTER FOR JUSTICE

Brennan Center for Justice at New York University School of Law
120 Broadway // 17th Floor // New York, NY 10271
www.brennancenter.org