BRENNAN
CENTER
FOR JUSTICE

*at New York University School of Law*

# A Procurement Guide for Better Election Cybersecurity

**by Christopher Deluzio**

## Introduction

Election officials across the country are turning their attention to procurement decisions about what equipment or services their jurisdiction might need going forward. Whether it's reviewing existing vendor relationships, considering new vendors for existing services, or even deciding whether to seek vendor support for something altogether new, officials face a bevy of difficult choices. The voting equipment and services jurisdictions purchase from vendors can have a substantial impact on the cybersecurity of elections, making these decisions quite consequential.

Vendors, of course, sell voting equipment — like optical scan systems, ballot-marking devices, and direct-recording electronic (DRE) machines — and the three largest sellers of voting machines account for more than 90 percent of this market.[1] But vendors also provide a range of other services and equipment, including e-pollbooks, election night reporting and tabulation systems, voter registration systems, ballot preparation services, and preelection logic and accuracy testing. As David Stafford, the supervisor of elections in Escambia County, Florida, told us, “The election vendors that we rely on are an integral part of election administration — they're critical.”[2]

In the face of growing cyber threats and the sophistication of adversaries, local election officials must deploy best practices in the selection and management of election vendors. To that end, this guide provides election officials and policymakers with steps they can take to ensure better cybersecurity from private election vendors.

## Recommendations

We look at seven key areas election officials and policymakers should consider as ways to achieve better vendor cybersecurity. These areas were selected based on the recommendations of election officials and cybersecurity experts we interviewed in the process of developing this guide, as well as our analysis of existing reports on the subject.

1. Source Code Disclosure
2. Robust Security Incident Reporting
3. Patching/Software Updates
4. Security Assessments/Audits
5. Regular Penetration Testing
6. Risk-Limiting Audit Support
7. Foreign Nexus Disclosure

In this guide, we provide language to implement these recommendations through (1) new laws or regulations, as well as (2) requests for proposals (RFPs) or contracts — drawing on examples from states and local jurisdictions across the country.

Of course, election security is a complicated topic involving dozens of considerations. This paper does not present an exhaustive list of vendor-related procurement best practices; rather it offers suggested language that jurisdictions can use (in law or contract) to ensure they are protected in the areas listed above.

Those interested in a more complete list of items they should consider before putting out an RFP or entering into a contract with a private vendor may want to consult a forthcoming procurement guide from the Center for Internet Security. The guide should be released in late spring 2019 and will include specific language election offices can use to increase the likelihood of positive outcomes in security.[3]

### 1. Source Code Disclosure

**Relevant vendor offerings: voting systems, e-pollbooks**

#### WHY IT MATTERS

Requiring vendors to disclose source code used in relevant software provides several key benefits to election officials, including increased transparency and the ability to independently audit and scrutinize code.

In a 2015 report, the Brennan Center advocated for disclosure of source code, highlighting New York's example of requiring vendors to permit the state to hold relevant code in escrow:

- "RFPs should provide jurisdictions with the right to maintain voting software. When New York State issued an RFP for new voting machines, it requested that the vendors permit the state to keep the system's source code in escrow. The state insisted on terms that would allow them to procure services from other vendors if the original vendor went out of business or was unresponsive to the needs of an election agency."[4]

Harvard's Belfer Center made similar recommendations in its February 2018 publication, *The State and Local Election Cybersecurity Playbook:*

- "Election officials should have access to the source code for any critical system to perform internal or third-party reviews. This can be a sensitive subject because of intellectual property concerns, but being able to independently audit vendor-created code allows officials to ensure that the code is secure. It also guarantees that the code does not contain any potentially unwanted networking requests, transfers of sensitive information, or modifications to key algorithms and counting mechanisms."[5]

#### ILLUSTRATIVE LANGUAGE

> Sample Legislative/Regulatory Language

Some states mandate by statute that vendors disclose source code for voting systems (something required under the U.S. Election Assistance Commission's existing testing and certification regime[6]). For example:

- California: "No later than 10 business days after the Secretary of State certifies or conditionally approves the use of a new or updated voting system, the vendor or county seeking certification or approval of the voting system shall cause an exact copy of the approved source code for each component of the voting system, including complete build and configuration instructions and related documents for compiling the source code into object code, to be transferred directly from either the United States Election Assistance Commission or the voting system testing agency that evaluated the voting system and is approved by the Secretary of State, and deposited into an approved escrow facility."[7]

- Colorado: (1) A voting system provider under contract to provide a voting system to a political subdivision in this state shall:…(b) Place in escrow with the secretary of state or an independent escrow agent approved by the secretary of state, immediately after the installation of election software, one copy of the state certified election software that was installed in each political subdivision, along with supporting documentation; (c) Place in escrow with the secretary of state any subsequent changes to the escrowed election software or supporting documentation."[8]

- New York: "Prior to the use of any voting machine or system in any election in the state,…the state board of elections and the local board of elections using such voting machine or system shall: 1. Require that the manufacturer and/or vendor of such voting machine, system or equipment shall place into escrow with the state board of elections a complete copy of all programming, source coding and software employed by the voting machine, system or equipment which shall be used exclusively for purposes authorized by this chapter and shall be otherwise confidential.[9]

### > Sample RFP/Contract Language

There may be situations where jurisdictions will want the flexibility to consider vendor offerings that provide disclosed source code (or open source offerings) against vendor offerings that do not provide such disclosures, particularly outside the voting systems context. For example, election officials will likely be best positioned to weigh the benefits of disclosure relative to other, competing offerings from vendors. In those situations, election officials would be wise to seek source code disclosure through the procurement process, rather than through legislation.

RFPs might, for instance, express a policy preference for open source systems (San Francisco's approach below) or mandate that vendors disclose relevant source code that is to be kept in escrow (which, as noted above, was New York's tactic). For example:

- San Francisco RFP (2015): "Further, the City has established a policy that gives preference to implementing voting systems designed using open source software. The City formally supports the development and eventual implementation of open source voting systems; thus, any organization or firm that has developed or is developing a voting system based on open source code, or intends to do so, and is moving, or, is preparing to move, its open source system through the certification processes is encouraged to reply to this RFI."[10]

- Volusia County, Florida (RFP 2015): "In the event the Contractor ceases to maintain experienced staff and the resources needed to provide any required software maintenance while under an obligation to provide such maintenance, the County shall be entitled to have, use, and duplicate for its own use, a copy of the source code and any other Software required for a fully operational recovery, along with all documentation for the software products covered by the Contract in order for the County to use the Software in accordance with the terms of the Contract."[11]

## 2. Robust Security Incident Reporting

**Relevant vendor offerings: all**

### WHY IT MATTERS

There is broad consensus that vendors should face mandatory security incident reporting to relevant election officials. This information is invaluable to those officials, arming them with timely information needed to identify and resolve problems. Incident reporting also gives officials key data about vendor performance, enabling a better assessment of the vendor relative to others during future bidding. Consequently, vendors will be incentivized to bolster their internal cybersecurity.

The National Academies of Sciences, Engineering, and Medicine's recent report, *Securing the Vote*, recommended mandatory vendor reporting of voter-registration-related issues both to customers and key governmental officials:

- "Vendors should be required to report to their customers, the U.S. Department of Homeland Security, the U.S. Election Assistance Commission, and state officials any detected efforts to probe, tamper with, or interfere with voter registration systems."[12]

The U.S. Department of Homeland Security included in its set of "evaluative questions and considerations when selecting vendors" an incident-reporting-related inquiry:

- "What conditions will trigger vendor reporting of cyber incidents to purchasers?"[13]

Others, including the Brennan Center,[14] have similarly called for vendor incident reporting:

- Belfer Center: "In your Service Level Agreements (SLAs), include clauses for vendors to notify you in the event of a cybersecurity breach of their systems or other unauthorized access immediately after they become aware and to cooperate with any consequential investigation, response, and mitigation."[15]

- Brookings Institution: "Election technology vendors should also be required to promptly report any discovered vulnerabilities to state election officials and the Department of Homeland Security."[16]

- Center for Internet Security: "The following terms should be considered for inclusion in the agreements in order to satisfy the identified information security requirements:…incident management requirements and procedures (especially notification and collaboration during incident remediation)."[17]

- Dwight Shellman, county regulation & support manager, Colorado Department of State: "Incidents that need to be reported can go beyond just a security breach and include hardware failure, unanticipated behavior of software, and behaviors that do not comport to description of software in user documentation. Incident reporting can be required as a condition of procurement, as condition of ultimate contract, or as a regulatory matter."[18]

- Eric Fey (Democratic director of elections, St. Louis County, Missouri): "If vendors aren't required to report security incidents, they won't. That's why it's critical to include this requirement in an RFP."[19]

ILLUSTRATIVE LANGUAGE

### > Sample Legislative/Regulatory Language

Mandatory incident reporting should be required of all election vendors in a state. For this reason, states should consider imposing this requirement through legislation. A federal bill from the prior Congress, the Secure Elections Act, provides useful language that mandates reporting within three days of discovery of an incident, while also requiring vendor cooperation with authorities.

*Secure Elections Act (S.2261)*:

- "If an 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, the election service provider shall—(1) 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 (2) cooperate with the election agencies in providing the notifications required under subsections (h)(1) and (i)."

- "The term 'election cybersecurity incident' means any information security incident involving an election system….The term 'incident' has the meaning given the term in section 3552 of title 44, United States Code,"[20] which defines "incident" as "an occurrence that—(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."[21]

Election rules in Colorado similarly mandate incident reporting and require notification of any voting system malfunction:

- "The voting system provider must submit a software or hardware incident report to the Secretary of State no later than 72 hours after a software incident has occurred."[22]

- "A vendor or designated election official must notify the Secretary of State within 24 hours of a reported or actual malfunction of its voting system. The notice must include a description, date, and the names of those who witnessed the malfunction, as well as the procedures followed before the malfunction, and any error messages displayed. The notice may be verbal, but a written notice must follow." [23]

### > Sample RFP/Contract Language

In addition, states may want to consider requiring the state's chief election officials to notify locals when she becomes aware of any security breach that could impact their systems.[24] Officials should memorialize in procurement the mandatory reporting obligation coupled with an obligation to cooperate with the jurisdiction, whether or not the requirement for security incident reporting exists in state law or regulation. Ohio provides a useful example that mandates reporting within 24 hours of a security breach (defined broadly) and cooperation with any subsequent investigation:

Ohio (RFP 2013):

- "In case of an actual security breach that may have compromised SOS Data, including but not limited to loss or theft of devices or media, the Contractor must notify the SOS in writing of the breach within 24 hours of the Contractor becoming aware of the breach, and fully cooperate with the SOS to mitigate the consequences of such a breach. This includes any use or disclosure of the SOS Data that is inconsistent with the Terms of this Agreement and of which the Contractor becomes aware, including but not limited to, any discovery of a use or disclosure that is not consistent with this Agreement by an employee, agent, or subcontractor of the Contractor. The Contractor must give affected the State full access to the details of the breach and assist each SOS in making any notifications to potentially affected people and organizations that the State deems are necessary or appropriate..." [25]

## 3. Patching/Software Updates

**Relevant vendor offerings: voting systems, e-pollbooks, voter registration databases, election-night reporting services**

### WHY IT MATTERS

Requiring vendors to provide software updates and patches will ensure that jurisdictions are using the most up-to-date software and that vendors are addressing improvements to software to address known vulnerabilities, weaknesses, bugs, and other issues. In that sense, this requirement reinforces an ongoing commitment to cybersecurity and software performance throughout the lifecycle of a contract — without requiring jurisdictions to foot the bill after initial procurement.

The Belfer Center, for instance, recommends mandatory patching and that officials consider patching practices when scrutinizing vendors:

- "Mandate patching as part of a vendor request for proposal (RFP) contract[] and ensure that the patching is conducted securely and frequently."[26]

- "Evaluate the levels of transparency associated with [vendors'] cybersecurity processes, and to what extent they will collaborate with you on key security risk-mitigation activities, including consequence management after a cyber incident. These would include…patching…."[27]

Similarly, the U.S. Department of Homeland Security recommends that election officials ask vendors to explain "patch management and update process" during the vendor selection phase:

- "What is the vendor's patch management and update process?"[28]

Doug Kellner, a co-chair of the New York State Board of Elections, suggested that jurisdictions retain the ability to seek upgrades and patches, as well as maintenance services, from vendors other than the original vendor:

"Contracts should not prevent counties from adding patching from a different vendor. By just having the option of a different vendor, it dampens the monopoly pricing power. For maintenance of voting machines, the vendor will often be the incumbent, but if the incumbent starts charging excessive pricing, then that invites competition. It's important that contract allows someone other than vendor to perform hardware maintenance on the machines."[29]

Amber McReynolds, former director of elections for Denver, Colorado, recommended that jurisdictions consider a 30-day pre-election "freeze window," where all but non-essential, security related patches and updates would be prohibited across all systems in the leadup to voting.[30]

### ILLUSTRATIVE LANGUAGE

> Sample RFP/Contract Language

Several jurisdictions have required mandatory software updates or patches through the procurement process. That approach makes sense given the unique nature of each specific procurement, and election officials we consulted endorsed this approach. Officials may want to include explicit language stating that the vendor shall provide these updates at no cost.

- Chicago (RFP 2017): "If Vendor or its subcontractors or manufacturers develops modifications, improvements, or upgrades to any part of the voting devices during the five-year warranty period, Vendor must provide them to the Board free of charge. Vendor must provide, at no additional cost, all new releases, upgrades and patches of the software during the warranty period. Documentation must be updated and delivered within ten (10) days after the new release or upgrade."[31]

- Jefferson County, Alabama (RFP 2015): "Successful bidder must provide warranty and maintenance coverage at no cost to the County the first year after final acceptance of system. Maintenance for the remainder of the contract term shall include routine maintenance, repairs of hardware/firmware and software malfunctions and provision of all system updates, including any security updates and patches."[32]

- Colorado (Contract 2006): "Contractor will, without charge to the State, correct any defects and make any additions, modifications or adjustments to any of the Deliverables or any update or revision to any software Deliverables as may be necessary to keep the Deliverables in operating order in accordance with specifications at all times in accordance with this Contract and the Statement of Work attached as Exhibit A."[33]

Edgardo Cortes, former Virginia commissioner of elections, noted that purchasing jurisdictions should make clear that "updates or patches should be subject to whatever testing and certification requirements are in place" to ensure that inserting updates or patches does not have unintended consequences on the security or reliability of the election system.[34]

In addition, with respect to voting systems, in particular, officials should be mindful of the U.S. Election Assistance Commission System Certification Process and applicable state laws that might limit when such patches can be implemented before elections.[35]

## 4. Security Assessments/Audits

**Relevant vendor offerings: all**

### WHY IT MATTERS

Election officials should require vendors to submit to security audits, either by government officials or third parties. Such assessments can provide officials with enhanced scrutiny of a vendor's cybersecurity practices, helping officials ensure vendor compliance with contractual and regulatory requirements.

The Center for Internet Security includes this suggestion — i.e., to subject vendors to outside audits — among its best practices for contracting with election vendors:

- "[A] best practice would be that the contractor is subjected to regular independent audits of security controls, with results available to the government organization. Elections officials may wish to have their own security audits. The contract will need to provide for this and the elections officials will need to set aside funds for the audits."[36]

And the Belfer Center similarly advises officials to retain the power to audit vendors and/or to subject vendors to third-party assessments:

- "State/local contracts with vendors should include provisions requiring vendors to conduct third-party vulnerability assessments of their systems and share the results."[37]

- "State officials should perform audits (and retain the right to do so) of a vendor's security practices and protocols. This activity provides assurance that the vendor's cybersecurity practices are robust and meet state and local security standards…."[38]

### ILLUSTRATIVE LANGUAGE

#### > Sample Legislative/Regulatory Language

Officials could consider implementing this recommendation either by statute or through the procurement process. By way of example, California's election code mandates governmental inspections and testing of voting systems:

- "The elections official of any county or city using a voting system shall inspect the machines or devices at least once every two years to determine their accuracy. Any county or city using leased or rented equipment shall determine if the equipment has been inspected for accuracy within the last two years before using it for any election. The inspection shall be made in accordance with regulations adopted and promulgated by the Secretary of State. The elections official shall certify the results of the inspection to the Secretary of State."[39]

- "The Secretary of State shall conduct random audits of the software installed on direct recording electronic voting systems…to ensure that the installed software is identical to the software that has been approved for use on that voting system. The Secretary of State shall take steps to ensure that the process for conducting random audits does not intentionally cause a direct recording electronic voting system to become more vulnerable to any unauthorized changes to the software that has been approved for its use."[40]

#### > Sample RFP/Contract Language

Officials looking to implement mandatory assessments/audits through procurement should consider the option to outsource assessments/audits to third parties while retaining the option of government personnel conducting such assessments/audits. Officials should also look to require vendor cooperation. The example below, from Colorado, does not explicitly address the state's ability to outsource to third parties, but officials may want to consider such language (which is suggested as an edit below in brackets).

- Colorado (RFP 2013): "Contractor shall permit the State, the federal government, and governmental agencies [as well as any third-parties acting on behalf of the State, the federal government, and/or governmental agencies] having jurisdiction, in their sole discretion, to monitor all activities conducted by Contractor pursuant to the terms of this Contract using any reasonable procedure, including, but not limited to: internal evaluation procedures, examination of program data, special analyses, on-site checking, formal audit examinations, or any other procedures. All monitoring controlled by the State shall be performed in a manner that shall not unduly interfere with Contractor's performance hereunder."[41]

## 5. Regular Penetration Testing

**Relevant vendor offerings: all**

### WHY IT MATTERS

Much like assessments of vendors' security practices, penetration testing of vendors should help to identify vulnerabilities before adversaries can exploit them. Here, as well, officials should retain the power to subject vendors to penetration testing by government officials and/or outside third parties.

Dwight Shellman of the Colorado Department of State told us that "it is absolutely essential that vendors consent to penetration testing of voting systems."[42] And Neal Kelley (Orange County, California's registrar of voters) stressed that Orange County has taken advantage of the Department of Homeland Security's vulnerability assessment services and that vendors should be subjected to similar scrutiny: "It doesn't make sense for us as a county to look at our vulnerabilities, then have a vendor's voting system with wide-open doors."[43]

The Brookings Institution has advocated for mandatory penetration testing as part of a broader regulatory regime around vendors:

- "Both federal and state governments must better regulate the commercial industry surrounding elections. Currently, this is a limited and proprietary market that too often leaves states with insufficient power to dictate security standards. In addition to setting standards for secure design, manufacturing, and storage of voting systems, the government must mandate ongoing processes such as routine penetration testing."[44]

The Belfer Center, which considers penetration testing "a critical element in ensuring that vulnerabilities in vendor environments are proactively identified and closed,"[45] advises officials to "[m]andate that vendors permit penetration testing of systems, including voting machines,"[46] through contracting:

- "The RFP should clearly include requirements for the vendor to allow penetration-testing by state officials or third parties of their systems to discover weaknesses. Vendors may resist these provisions, especially if they hold broader state contracts that could be affected if vulnerabilities are discovered. Nonetheless, conducting these tests represents the best way to identify cracks in critical infrastructure before malicious actors do, and should be part of any contract with vendors who work on and maintain these systems."[47]

### ILLUSTRATIVE LANGUAGE

Memorializing this recommendation will likely overlap with the above recommendation to mandate assessments/security audits of vendors. Much of the illustrative language for that recommendation will also be useful here.

#### > Sample Legislative/Regulatory Language

Officials considering a statutory approach may also want to consider the Secure Elections Act, which would institute a "Hack the Election" program to "identify and report election cybersecurity vulnerabilities."[48]

*Secure Elections Act (S.2261)*:

- "In establishing the program required under subsection (a), the Secretary shall—(1) establish a recurring competition for independent technical experts to assess election systems for the purpose of identifying and reporting election cybersecurity vulnerabilities; (2) establish an expeditious process by which independent technical experts can qualify to participate in the competition; (3) establish a schedule of awards (monetary or non-monetary) for reports of previously unidentified election cybersecurity vulnerabilities discovered by independent technical experts during the competition; (4) establish a process for election agencies and election service providers to voluntarily participate in the program by designating specific election systems, periods of time, and circumstances for assessment by independent technical experts; and (5) promptly notify election agencies and election service providers about relevant election cybersecurity vulnerabilities discovered through the competition, and provide technical assistance in remedying the vulnerabilities."[49]

#### > Sample RFP/Contract Language

Illustrative RFPs include specific mention of "penetration tests" or "hacking vulnerability testing," which should leave little doubt about what is expected of vendors in this regard:

- Colorado (RFP 2013): "Security personnel and administrators will audit systems access, review system and application logs, search for security violations, monitor Internet traffic, perform systems penetration tests, and carry out other security related functions on all systems on a regular basis as permitted by the Chief Information Officer (CIO)."[50]

- Pima County, Arizona (RFP 2014): "The system shall have the capability to permit diagnostic testing of all the major components. Vendor shall include documentation for electronic intrusion and software modification or hacking vulnerability testing."[51]

## 6. Risk-Limiting Audit Support

**Relevant vendor offerings: voting systems, ballot preparation, and design services**

### WHY IT MATTERS

There is wide consensus that the most secure type of voting employs voting systems that rely on voter-marked, human-readable paper ballots.[52] This paper-based voting must, however, be accompanied by audits of the ballots.

Best practice is to conduct statistically sound, robust post-election audits of voter-marked paper ballots after every election, and experts consider risk-limiting audits to be the "gold standard" of post-election audits.[53] Such audits have the benefit of providing a high likelihood of identifying an error in tabulation of votes affecting the outcome, while providing an efficiency advantage over traditional audits that tend to require officials to sample a fixed percentage or number of ballots, regardless of margin of victory.[54]

For example, the National Academies' recent report, *Securing the Vote,* recommended that states "mandate risk-limiting audits prior to the certification of elections," something that "requires the use of paper ballots."[55] To do so, voting systems must be able to match cast vote records (CVRs) to ballots cast — the CVR is the "[a]rchival record of all votes produced by a single voter" and can "be in electronic, paper, or other form."[56] According to the National Academies' report:

- "States and jurisdictions purchasing election systems should consider in their purchases whether the system has the capacity to match CVRs to physical ballots, as this feature could result in future cost savings when audits are conducted."[57]

This requirement, which will also require either imprinting ballots with a unique identifier corresponding to the CVR or segregating ballots by scanner, will facilitate a potentially cost-effective form of risk-limiting audits called *comparison audits*. An EAC report lauds the potential efficiency gains of comparison audits:

- "The comparison RLA provides efficiency by allowing election officials to compare a ballot to the voting system's CVR and generally allows jurisdictions to audit fewer ballots compared to other audit methods."[58]

### ILLUSTRATIVE LANGUAGE

#### > Sample Legislative/Regulatory Language

Several states already mandate risk-limiting audits by statute, which election officials can consult when looking to mandate such audits. Requiring that the audits occur before certification is important to maximizing the utility and effectiveness of the audits, as is making clear that the results of any full recount would replace any unofficial results.

Colorado

- "(2)(a) Commencing with the 2017 coordinated election and following each primary, general, coordinated, or congressional vacancy election held thereafter, each county shall make use of a risk-limiting audit in accordance with the requirements of this section. Races to be audited shall be selected in accordance with procedures established by the secretary of state, and all contested races are eligible for such selection….
- (4) The secretary of state shall promulgate rules in accordance with article 4 of title 24, C.R.S., as may be necessary to implement and administer the requirements of this section. In connection with the promulgation of the rules, the secretary shall consult recognized statistical experts, equipment vendors, and county clerk and recorders, and shall consider best practices for conducting risk-limiting audits.
- (5) As used in this section: …(b) 'Risk-limiting audit' means an audit protocol that makes use of statistical methods and is designed to limit to acceptable levels the risk of certifying a preliminary election outcome that constitutes an incorrect outcome."[59]

Rhode Island

- "(b) Commencing in 2018, the board, in conjunction with local boards, is authorized to conduct risk-limiting audits after all statewide primary, general, and special elections in accordance with the requirements of this section. Commencing in 2020, the state board, in conjunction with local boards, must conduct risk-limiting audits after the presidential preference primary and general elections in accordance with the requirements in this section….
- (d) If a risk-limiting audit of a contest leads to a full manual tally of the ballots cast using the voting system, the vote counts according to that manual tally shall replace the vote counts reported pursuant to §§ 17-19-36 and 17-19-37 for the purpose of determining the official contest results pursuant to §§ 17-22-5.2 and 17-22-6."[60]

#### > Sample RFP/Contract Language

Rather than stating detailed requirements about CVRs and imprinting capabilities, which might run into state ballot secrecy issues, officials might consider employing language to straightforwardly require that voting systems support ballot-level comparison audits:

- "The voting system shall support ballot-level comparison audits of individual paper ballots, consistent with applicable law and regulations."

### 7. Foreign Nexus Disclosure

**Relevant vendor offerings: all**

WHY IT MATTERS

Foreign efforts to interfere in American elections, including Russian attacks on the nation's election infrastructure, continue to garner attention. These threats highlight the importance of election officials understanding whether vendors might be presenting avenues of attack for foreign adversaries.

Just this past summer, for example, the FBI notified Maryland officials that a vendor servicing the state's voter registration database, online voter registration system, and election night reporting website, among other things — ByteGrid LLC — had substantial ties to Russia.[61] Specifically, the FBI informed Maryland officials that the vendor's financing source (AltPoint Capital Partners) had as its largest investor Russian oligarch Vladimir Potanin. The vendor had not disclosed this foreign ownership to Maryland officials — a fact that would have been critically important to assessing whether the vendor's cybersecurity was adequate for Maryland.[62]

This example highlights the importance of election officials being aware of any foreign ownership, control, or influence affecting a vendor. According to Eric Fey, the St. Louis County, Missouri, Democratic director of elections, "It's important to require vendors to disclose foreign ownership and entanglement so that the [election official] can make their own cost/benefit analysis."[63] But requiring such disclosure is insufficient if not coupled with a requirement for vendors to disclose promptly any changes that might affect a vendor's foreign entanglements.

ILLUSTRATIVE LANGUAGE

> Sample Legislative/Regulatory Language

There have been several bills pending in Congress seeking to regulate vendors' foreign ties — local election officials could consider the approaches of these bills in drafting language to mandate vendor disclosure of fore ign ties, particularly in the event that Congress does not pass such a measure. Election officials could also incorporate similar language into RFPs if necessary.

For example:
*Election Vendor Security Act (H.R. 6435)*:

- "(1) The vendor shall 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 (as defined in section 1(b) of the Foreign Agents Registration Act of 1938 (22 U.S.C. 611(b)), or by any agent of a foreign principal required to register under such Act.

- (2) The vendor shall disclose to the Chair and the Secretary, and to the chief State election official of any State in which the vendor provides, supports, or maintains any component of an election system, any sourcing outside the United States for parts of the system." [64]

*Protect Election Systems from Foreign Control Act (H.R. 6449)*

- Defining "qualified voting system vendor" as a vendor who meets several criteria, including:

- "(A) Except as provided in paragraph (2), the person is solely owned and controlled by a citizen or citizens of the United States.

- (B) The person discloses any sourcing outside the United States for any parts of the voting system to the Chair of the Commission, the Secretary of Homeland Security, and the chief State election official of any State in which the vendor provides or seeks to provide goods or services with respect to the voting system.

- (C) The person discloses any material change in its ownership or control to the Chair of the Commission, the Secretary of Homeland Security, and the chief State election official of any State in which the vendor provides goods or services with respect to the voting system."[65]

The bill also permits a waiver of the domestic ownership requirement:

- "The Secretary of Homeland Security may waive the requirement of subparagraph (A) of paragraph (1) with respect to a person who is a United States subsidiary of a parent company which has implemented a foreign ownership, control, or influence mitigation plan that has been approved by the Secretary. Such plan shall ensure 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."[66]

## Additional Suggestions

Our interviews with election officials and other experts produced two more suggestions that jurisdictions may want to consider when entering into new agreements with private vendors. First, suggests Amber McReynolds, former director of elections for Denver, Colorado, "Having a security agreement and communication plan between vendors and election officials for each election," which would detail things like support structure, reporting, and contact requirements.[67] This could also be used to confirm background checks for vendor employees.

Second, Matthew Davis, former chief information officer for Virginia's Department of Elections, suggests conducting baseline testing on all equipment upon receipt and prior to every deployment. These test results can be used to confirm that the equipment received is delivered as ordered. They can also be used for comparison purposes after an election if any concerns are raised during an election.

## Conclusion

The combination of aging infrastructure and heightened attention to election security means that there will likely be a large number of purchases of election systems and services around the country, unmatched perhaps since the years following the passage of the Help America Vote Act in 2002. The knowledge election officials and others have gained in that time provides us with a unique opportunity to reset the clock and ensure that private vendors who play a central and critical role in American elections are delivering products and services that will increase the security of those elections.

## Endnotes

1 Lorin Hitt, Simran Ahluwalia, Matthew Caulfield, Leah Davidson, Mary Margaret Diehl, Alina Ispas, and Michael Windle, *The Business of Voting: Market Structure and Innovation in the Election Technology Industry*, Penn Wharton Public Policy Initiative, 2017, 23, https://trustthevote.org/wp-content/uploads/2017/03/2017-whartonoset_industryreport.pdf.

2 David Stafford, (supervisor of elections, Escambia County Florida), interview by the Brennan Center for Justice, December 17, 2018.

3 When posted, the guide will be available here: https://www.cisecurity.org/ei-isac/.

4 Lawrence Norden and Christopher Famighetti, *America's Voting Machines at Risk*, Brennan Center for Justice, 2015, 37, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

5 Meredith Berger, Charles Chretien, Caitlin Conley, Jordan D'Amato, Meredith Davis Tavera, Corinna Fehst, Josh Feinblum, Kunal Kothari, Alexander Krey, Richard Kuzma, Ryan Macias, Katherine Mansted, Henry Miller, Jennifer Nam, Zara Perumal, Jonathan Pevarnek, Anu Saha, Mike Specter, and Sarah Starr, *The State and Local Election Cybersecurity Playbook*, Harvard Kennedy School and Defending Digital Democracy, 2018, 51, https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf.

6 *See, e.g., Voting System Testing and Certification Program Manual, Version 2.0,* U.S. Election Assistance Commission, 2015, https://www.eac.gov/assets/1/28/Cert.Manual.4.1.15.FINAL.pdf.

7 Cal. Elec. Code § 19212.

8 Colo. Rev. Stat. Ann. § 1-7-512.

9 N.Y. Elec. Law § 7-208.

10 Department of Elections, City and County of San Francisco, Request for Information:
The City and County of San Francisco's Voting System (California, 2015), https://www.eac.gov/assets/1/28/SF_RFI_VotingSystem.pdf.

11 Department of Elections, Volusia County, Request for Proposal for Voting System, (Florida, 2015), https://www.eac.gov/assets/1/28/1.) 15-P-66PW_Voting_System_RFP_FINAL.pdf.

12 *Securing the Vote: Protecting American Democracy,* The National Academies of Sciences, Engineering, and Medicine, 2018, 5, https://www.nap.edu/read/25120/chapter/1.

13 National Protection and Programs Directorate, *DHS Election Infrastructure Security Funding Consideration*, Department of Homeland Security, 2018, 5, https://www.dhs.gov/sites/default/files/publications/Election%20Infrastructure%20Security%20Funding%20Considerations%20Final.pdf.

14 *See, e.g.,* Lawrence Norden,*Voting System Failures: A Database Solution,* Brennan Center for Justice, 2010, 32, http://www.brennancenter.org/sites/default/files/legacy/Democracy/Voting_Machine_Failures_Online.pdf ("We propose that the government require all vendors to provide written notification via certified mail…when they determine that a voting system failure or vulnerability may exist….").

15 Berger, Chretien, Conley, D'Amato, Davis Tavera, Fehst, Feinblum, Kothari, Krey, Kuzma, Macias, Mansted, Miller, Nam, Perumal, Pevarnek, Saha, Specter, and Starr, *The State and Local Election Cybersecurity Playbook,* 50.

16 *Cybersecurity of Voting Machines: Hearings on H.R., Before the Committee on Oversight and Government Reform*, 115th Cong. (2017) (statement of Susan Hennessey, fellow of National Security Law in Governance Studies at the Brookings Institution and executive editor of *Lawfare*), https://www.brookings.edu/testimonies/cybersecurity-of-voting-machines/.

17 Brian Calkin, Kelvin Coleman, Brian de Vallance, Thomas Duffy, Curtis Dukes, Mike Garcia, John Gilligan, Paul Harrington, Caroline Hymel, Philippe Langlois, Adam Montville, Tony Sager, Ben Spear, and Roisin Suver, *A Handbook for Elections Infrastructure Security,* Center for Internet Security, 2018, 65, https://www.cisecurity.org/wp-content/uploads/2018/03/CIS-Elections-Handbook-19-March-Single-Pgs.pdf.

18 Dwight Shellman (county regulation and support manager, Colorado Secretary of State's Office), interview by the Brennan Center for Justice, Decem-

ber 13, 2018.

[19] Eric Fey (Democratic Director of Elections, St. Louis County, Missouri), interview by the Brennan Center for Justice, December 3, 2018.

[20] Secure Elections Act, S.2261,115th Cong. (2017–2018).

[21] 44 U.S.C. § 3552(b)(2).

[22] Colo. Code Regs. 1505-1:11, Rule 11.7.1 (2018)

[23] Colo. Code Regs. 1505-1:11, Rule 11.7.2 (2018)

[24] Amber McReynolds, (former elections director, Denver, Colorado), email message to Lawrence Norden, February 7, 2019.

[25] Department of Administrative Services, State of Ohio, Request for Proposals: UOCAVA Ballot Delivery & Tracking System, (Ohio, 2013), https://www.eac.gov/assets/1/28/Ohio2%20-%2010.10.13%20-%20RFP%200A1120.pdf.

[26] Berger, Chretien, Conley, D'Amato, Davis Tavera, Fehst, Feinblum, Kothari, Krey, Kuzma, Macias, Mansted, Miller, Nam, Perumal, Pevarnek, Saha, Specter, and Starr, *The State and Local Election Cybersecurity Playbook*, 48.

[27] Ibid., 49.

[28] *DHS Election Infrastructure Security Funding Consideration*, 2018, 7.

[29] Doug Kellner (co-chair, New York State Board of Elections), interview by the Brennan Center for Justice, December 17, 2018.

[30] Amber McReynolds (former elections director, Denver, Colorado), interview by the Brennan Center for Justice, December 20, 2018.

[31] Board of Election Commissioners, Chicago, Request for Proposals: Voting System (Illinois, 2017), https://app.chicagoelections.com/documents/general/Voting-Equipment-RFP-2017-07-07.pdf.

[32] Purchasing Division, Jefferson County Commission, Request for Proposal: Electronic Voting Counting System (Precinct Tabulator Equipment), (Alabama, 2015), https://www.eac.gov/assets/1/28/Jefferson County, AL 100-15 Electronic Voting Counting System.docx.

[33] Colorado Department of State and Saber Software, Inc., Statewide Colorado Registration and Election (SCORE II) Contract, (Colorado, 2006), https://www.sos.state.co.us/pubs/elections/SCORE/files/SCOREIIcontractwithcorrectionsoct2006.pdf.

[34] Edgardo Cortes, former commissioner of elections, Virginia (email message to Lawrence Norden, February 7, 2019).

[35] *See EI-ISAC Cybersecurity Spotlight – Patching,* Center for Internet Security, https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-patching/.

[36] Calkin, Coleman, de Vallance, Duffy, Dukes, Garcia, Gilligan, Harrington, Hymel, Langlois, Montville, Sager, Spear, and Suver, *A Handbook for Elections Infrastructure Security,* 33.

[37] Berger, Chretien, Conley, D'Amato, Davis Tavera, Fehst, Feinblum, Kothari, Krey, Kuzma, Macias, Mansted, Miller, Nam, Perumal, Pevarnek, Saha, Specter, and Starr, *The State and Local Election Cybersecurity Playbook*, 48.

[38] Ibid., 51.

[39] Cal. Elec. Code § 19230.

[40] Cal. Elec. Code § 19233.

[41] Department of State, State of Colorado, Request for Proposal: Uniform Voting System, (Colorado, 2013), https://www.eac.gov/assets/1/28/Colorado%20Uniform%20Voting%20System%20RFP%202013_10_01.pdf.

[42] Dwight Shellman (county regulation and support manager, Colorado Secretary of State's Office), interview by the Brennan Center for Justice, December 13, 2018.

[43] Neal Kelley (registrar of voters, Orange County California), interview by the Brennan Center for Justice, December 20, 2018.

[44] *Cybersecurity of Voting Machines: Hearings on H.R., Before the Committee on Oversight and Government Reform*, (statement of Susan Hennessey).

[45] Berger, Chretien, Conley, D'Amato, Davis Tavera,

Fehst, Feinblum, Kothari, Krey, Kuzma, Macias, Mansted, Miller, Nam, Perumal, Pevarnek, Saha, Specter, and Starr, *The State and Local Election Cybersecurity Playbook*, 51.

46 Ibid., 48.

47 Ibid., 51.

48 Secure Elections Act, S.2261, 115th Cong. (2017-2018).

49 Ibid.

50 Department of State, State of Colorado, Request for Proposals: Statewide Electronic Pollbook System (Colorado, 2013), https://www.eac.gov/assets/1/28/RFP%20CDOS-EPOLL-1%20-%20Request%20for%20Proposals%20-%20Document%201%20of%203.pdf.

51 Procurement Department, Pima County, Notice of Request for Proposals: Elections Voting System and Related Services, (Arizona, 2014), https://www.eac.gov/assets/1/28/Pima%20County.AZ-rfp.pdf.

52 *Securing the Vote: Protecting American Democracy,* 6-7; "Paper Ballots," Election Technology, National Election Defense Coalition, https://www.electiondefense.org/paper-ballots/ ("Public hand counting of voter marked paper ballots is the only system that allows for full citizen oversight of elections — the foundation of democratic self-governance.").

53 Lawrence Norden and Wilfred U. Codrington III, "America's Voting Machines at Risk — An Update," Brennan Center for Justice, March 8, 2018, https://www.brennancenter.org/analysis/americas-voting-machines-risk-an-update.

54 Christopher Deluzio, "A Smart and Effective Way to Safeguard Elections," Brennan Center for Justice, July 25, 2018, https://www.brennancenter.org/blog/smart-and-effective-way-safeguard-elections.

55 *Securing the Vote: Protecting American Democracy*, 101.

56 Jerome Lovato, *Risk-Limiting Audits — Practical Application,* U.S. Election Assistance Commission, 2018, 4, https://www.eac.gov/assets/1/6/Risk-Limiting_Audits_-_Practical_Application_Jerome_Lovato.pdf.

57 *Securing the Vote: Protecting American Democracy*, 100.

58 Lovato, *Risk-Limiting Audits — Practical Application*, 5.

59 Colo. Rev. Stat. §1-7-515.

60 17 R.I. Gen. Laws Ann. § 17-19-37.4.

61 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.

62 Ibid.

63 Eric Fey (Democratic director of elections, St. Louis County, Missouri), interview by the Brennan Center for Justice, December 3, 2018.

64 Election Vendor Security Act, H.R.6435, 115th Cong. (2017-2018).

65 Protect Election Systems from Foreign Control Act, H.R.6449, 115th Cong. (2017-2018).

66 Ibid.

67 Amber McReynolds, (former elections director, Denver, Colorado), email message to Lawrence Norden, February 7, 2019.

## Acknowledgments

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

The author gratefully acknowledges the colleagues who collaborated in preparing this report. Brennan Center Deputy Director Lawrence Norden provided instrumental guidance, direction and edits. Research and Program Associate Andrea Cordova offered research assistance and handled interview logistics. Counsel Liz Howard provided thoughtful suggestions and feedback.

The Brennan Center is also immensely grateful for the many experts and officials whose knowledge and views helped shape this report. We sincerely thank the following individuals for generously sharing their expertise and information through interviews: Mike Garcia, senior advisor for elections best practices, Center for Internet Security; Dwight Shellman, county regulation and support manager, Colorado Secretary of State's Office; Doug Kellner, co-chair, New York State Board of Elections; Dean Logan, registrar-recorder/county clerk, Los Angeles County California; Noah Praetz, director of elections, Cook County, Illinois; Maggie Toulouse Oliver, secretary of state, New Mexico; Rokey Suleman, former elections director, Richland County, South Carolina; Chris Thomas, former elections director, Michigan; Neal Kelley, registrar of voters, Orange County, California; Brenda Cabrera, director of elections, City of Fairfax, Virginia; Kammi Foote, registrar of voters, Orange County, California; Amber McReynolds, executive director, National Vote at Home Institute; Eric Fey, Democratic director of elections, St. Louis County, Missouri; and David Stafford, supervisor of elections, Escambia County, Florida.

This report also benefitted from individuals willing to share their valuable experience and provide insight in the review process. Alongside many of the aforementioned experts, we gratefully acknowledge the following for their helpful feedback: Edgardo Cortes, former commissioner of elections, Virginia, and current election security advisor, Brennan Center; and Matthew Davis, former chief information officer of Virginia's Department of Elections.

The proposals, views, and recommendations in this report — as well as any mistakes — should be attributed only to the author.