OSET INSTITUTE

Election Technology Briefing

Version 3

Moving the Needle on Voting System Updates

Improving the Process as a Matter of National Security

Prepared for:

U.S. Election Administrators, Public Policy Leadership & Interested Citizens

Prepared By:

Edward Perez

Global Director, Technology Development

Contribution From:

Gregory Miller

Co-Founder, Chief Operating Officer

August 2019

Introduction

With the start of primary season for the Presidential Election right around the corner, in February 2020, the security of U.S. election infrastructure remains a topic of national concern. As recently as April 2019, FBI Director Christopher Wray observed[1] that *"…our adversaries are going to keep adapting and upping their game, and so we're very much viewing 2018 [elections] as just kind of a dress rehearsal for the big show in 2020."*

The current state of U.S. voting systems in particular has been scrutinized even more closely, and a recent Associated Press story[2] noted that "*the vast majority of 10,000 election jurisdictions nationwide use Windows 7 or an older operating system to create ballots, program voting machines, tally votes and report counts.*" Given the fact that Microsoft will no longer provide free, regular updates to Windows 7 users after January 2020 (known as "end of support"), reports of outdated voting system software with potential vulnerabilities have garnered a lot of attention.

Many observers are asking the reasonable question, "*Can't we simply get everything updated before the 2020 elections*?" The short answer, unfortunately, is "No" — due to a complex set of limitations associated with how voting system software is developed, certified, sold, implemented, and maintained. Until now, those complexities have not been explained in plain language for the benefit of citizens, voters, and other interested parties, and here, we hope to change that.

---

1 See: https://www.apnews.com/e127a2b9880f16970b5eb6acd1fb7678

2 See: https://www.apnews.com/e5e070c31f3c497fa9e6875f426ccde1

The purpose of this Briefing is to shed light on the process of how voting systems are purchased, deployed, and updated, with a special emphasis on the challenges that currently prevent more flexible software updates. We hope that by illuminating what all of this means for election administrators, vendors, and the nation as a whole, policy makers can better understand what needs to change to ensure the security of the nation's election infrastructure in the future.

It's not a simple story to tell, so settle in for a journey of insight. Along the way, we address:

- What's typically included in a voting system purchase;
- Typical industry policies around software upgrades;
- How upgrades are implemented;
- The reasons for the challenges that exist today; and
- Recommendations for how things might be improved in the future.

The bottom line is, the current workflows aren't working, and the security of our voting infrastructure is suffering as a result. Thus, the OSET Institute offers the following Briefing on this issue authored by our *Global Director of Technology Development*, Eddie Perez. Mr. Perez's extensive 15-year industry experience enables the Institute to produce a deep look into the issues that we hope will make this a valuable resource for policy makers in particular.

1. What Does a Voting System Purchase Typically Include?

When states, counties, or townships purchase a new voting system, the transaction usually involves two (2) different "buckets" of cost – capital expenses incurred at the time of initial purchase, and operating expenses apportioned over several years through annual fees labeled as "support and maintenance." Let's look at each.

Bucket #1: The Tangibles: Physical Assets

We begin with the tangible "things" that election jurisdictions typically pay for at the time of the initial purchase: the voting system components that are delivered to a warehouse. Voting systems include a combination of hardware and software. Hardware typically includes desktop computers that back-office election staff uses to design elections and tabulate votes; and also the voting devices themselves, (e.g., ballot scanners, ballot marking devices, or other electronic voting machines for in-person voting; and high-speed scanners for jurisdictions with a lot of by-mail voting).

In addition to the hardware, every piece of equipment also includes software that allows it to perform its functions; the installed software is a combination of "commercial off-the-shelf" (COTS) software designed for "mainstream," non-voting specific applications (e.g., Microsoft operating system software (OSS)) are common, *plus* additional proprietary software (commonly called the "election management system," or EMS), which the voting system manufacturer develops and integrates with the operating system.

It's important to note that when an election jurisdiction takes delivery of voting system hardware and software, it typically "owns" only the hardware itself. The jurisdiction does not "own" the software installed on the devices, however; instead, it has a "right to use" the software, which is granted through payment of a "license" for each instance of the software installed.

For example, in addition to the cost of a computer, a back-office EMS desktop PC may include the cost of an operating system license, plus a license to use the vendor's ballot design or tabulation software, which is also installed on the PC; and each voting device would also require a license for its installed software, in addition to the cost of the device itself.

To illustrate a simplified "bill of sale" for a new voting system purchase, it might include the following hardware and software (*among other things*):

Description	Qty	Unit Price	Extended Price	Comments
Ballot design desktop PC	1	$20,000	$20,000	For back-office election staff; used to create elections
Tabulation desktop PC	1	$15,000	$15,000	For back-office election staff; used to count votes and report results
Polling place scanner	10	$5,500	$55,000	For voters, to cast their marked paper ballots
Accessible ballot marking device	10	$3,500	$35,000	For voters with disabilities, who cannot hand-mark ballots
Year 1 software license for each component	1 per device	Included	Included	No additional charge for Year-1
	Total Initial Purchase:		**$125,000**	

Why does the distinction between hardware and software matter? The fact that election jurisdictions only have a "right to use" software license through payment of a license fee – but they do *not "own"* the software — means that although they may take ownership possession of election devices (assuming a purchase versus an equipment lease), they must continue paying fees, year after year (for a long as their contract with the voting system vendor lasts), in order to continue using the software installed on the voting components they may now own. Those fees lead us to the second type of cost item associated with a voting system purchase: Annual Fees.

Bucket #2: The Intangibles: Annual License & Support Fees

As noted in the example above, when an election jurisdiction purchases a new voting system, the hardware it acquires (through purchase or lease) typically includes licenses for all installed software for *only* the *first year* of ownership. After year-1, service models in the voting industry typically require jurisdictions to pay annual fees in order to have continued access to various benefits. Those fees are typically known as "License & Support Fees." License and support fees provide customers with the continued right to use the installed voting system software (on back-office EMS computers, as well as on individual voting devices), and they help to offset the costs that vendors incur to provide services such as online and telephone support; ongoing documentation (such as product bulletins and/or training updates); and development of future software updates, which are made available to jurisdictions that are current on payment of their annual fees.

A simplified example of "license and support" annual maintenance fees might look like the table below. Again, although the first year software license fees *were included* with the initial equipment purchase, Years 2-5 (four (4) additional years) require the election jurisdiction to

continue paying annual fees in order to legally continue using the voting system and to have access to any future software updates.

Description	Term	Price per PC or voting device	Qty	Annual Fee	Extended Price, Years 2-5 Total
Software license & support – Ballot design desktop PC	Years 2-5	$20,000	1	$20,000	$80,000
Software license & support - Tabulation desktop PC	Years 2-5	$15,000	1	$15,000	$60,000
Firmware license & support - Polling place scanner	Years 2-5	$100	10	$1,000	$4,000
Firmware license & support - Accessible ballot marking device	Years 2-5	$75	10	$750	$3,000
				Total – License & Support, 4 Additional Years:	**$147,000**

Importantly, license and support fees are *in addition to* the Year-1 equipment acquisition (purcahse or lease) costs previously described. Furthermore, bear in mind that license and support fees can add up, *quickly*. In this example, note that over the remaining 4-years of this hypothetical contract term, the total cost of annual license and support fees is *even more than* the amount the election jurisdiction spent to initially procure all of its voting equipment (i.e., in this example, $125,000 initial vs. $147,000 for four additional years).

With all that in mind, it's easy to see how these license and support fees, which lead to recurring annual revenue for voting system manufacturers, can be significant. These "revenue streams" are the lifeblood for vendors, and given their cost, they should provide demonstrative ongoing benefits for election jurisdictions. Especially important, these same fees support future product development, including software updates.

So what's the story with updates? Why might software updates be necessary? And who gets to decide when and how they are released?

2. When Might Updates to Voting System Occur?

After voting system manufacturers implement voting systems in an election jurisdiction, that jurisdiction typically uses the same voting system for many years – up to a decade, and practically speaking, often longer. During that time, if updates are made available from the voting system manufacturer, they are typically released for one or more of the following reasons:

1. To offer users new value-added features and functionality (e.g., improvements that make election management easier, or more efficient, or that increase the performance of the voting system).
2. To correct system defects (e.g., "bug fixes").
3. To comply with changes in federalor state law or administrative rules, so that the voting system can perform mandated functions.

4. To mitigate supply chain concerns, by updating COTS software or hardware (e.g., operating system software, scanners, or printers) that is no longer supported, or which cannot be easily sourced.

More specifically, here are some examples of actual "updates" that one or more major voting system vendors have offered in recent years:

- To introduce new types of voting devices that the vendor previously did not offer, such as newly-designed "hybrid" ballot marking devices.
- To comply with state-specific rules for certain types of voting variations (e.g., such as particular ways of tabulating straight party votes, or special rules around entering write-in votes).
- To increase the "system limits" and foreign language capabilities of the voting system, so that it is suitable for use by very large jurisdictions with many districts, precincts, contests, and ballot styles.
- To update the underlying COTS operating system software on devices comprising the voting system (e.g., updating from Windows 7 to Windows 10)

All of those are pretty straightforward reasons for potentially updating voting systems, but uncertainties about their actual development and deployment arise, primarily for two reasons:

1. Vague contract language. Unless election jurisdictions push back against the typical "default" contracts that vendors offer, contractual language about updates is usually quite murky; and
2. Unequal contract language. The contractual language about updates that *does* exist usually increases the power and discretion of vendors to release updates *only when they choose to do so*.

Below are three examples of representative contract language about updates from each of the major vendors, based on actual "Master Agreements" or "General Terms," available from public sources on the Internet (e.g., government procurement departments). It should be emphasized that in each example below, *the brief paragraphs represent the full extent of contract language about updates; there are typically no additional details anywhere else in the contract*— and as you can read, the language often lacks specificity. Emphasis has been added, where applicable.

Contract Example #1 – Updates from Voting System Vendor A

> *Upgrades. In the event that Vendor, at its sole discretion, certifies a software upgrade under the applicable provisions of the election laws and regulations of the Licensee's State, Vendor may make the certified software upgrade available to the Licensee [e.g. the election jurisdiction] and install the upgrade during a regularly schedule preventive maintenance as described in Exhibit A.*

Contract Example #2 – Updates from Voting System Vendor B

> *Software Support Services may consist of periodic updates to Vendor's Proprietary Software, at Vendor's discretion. Because not all errors or defects can or need to be corrected, Vendor does not warrant that all errors or defects will be corrected. Software errors or defects must be reported in writing and be accompanied with sufficient detail to*

enable Vendor staff to reproduce the error and provide a remedy or suitable corrective action. The exclusions from warranty coverage under Section 9.5 also are exclusions from Software Support Services under this Section. There may be consumable, shipping and on-site service charges for update releases of software and there may be feature charges for update or enhancement releases of software.

Contract Example #3 – Updates from Voting System Vendor C

During the Software Maintenance and Support Term, Vendor may provide new releases, upgrades or maintenance patches to the Software, along with appropriate documentation ("Updates"), on a schedule solely defined by Vendor. Customer is responsible for obtaining and installing any upgrades or purchases of third party hardware or software required to operate the Updates. Customer may install the Updates in accordance with Vendor's recommended instructions or may request that Vendor install the Updates. Vendor will charge Customer separately to (a) deliver the Updates, (b) train customer on the use of such Updates, and (c) provide maintenance and support on the Software, which is required as a result of Customer's failure to timely install an Update. Customer shall pay Vendor for any Update, which is required due to a change in state law.

The key takeaways about voting system updates, illustrated in these examples, are:

- Typical contracts leave it up to the sole discretion of vendors—*not election jurisdictions*—to decide whether and when software updates will be developed and made available.
- Typical (i.e., "default" or "boilerplate") contract language is vague, with few restrictions placed on voting system vendors.
- There may be additional costs associated with vendor provision of updates to customers, *beyond those covered through annual license and support fees* (though this is often unclear); such charges may include, for example, costs of development, shipping, and installation.

Not surprisingly, since typical contracts increase vendor discretion at the expense of local election officials, at best it is not uncommon for local election officials to be relatively unclear about when their voting systems might be updated, or what it might cost them to do so. At worst, customers might pay considerable annual license and support fees that provide few benefits beyond a right to use software, and telephonic support. Indeed, some users of older voting systems have had to live with software that their vendor has chosen not to update *at all* for a decade or more.

Why are local election officials often so relatively powerless? And why might voting system vendors resist making more frequent updates? A big part of the answer lies in the complexities of what's actually required to release and implement an updated version of voting system software. Under the current environment, it's *not* easy.

3. What's Required to Implement Voting System Updates?

Assuming that a vendor actually agreed to develop, test, and release updated software for a voting system, implementing the update is *far* more complicated than what mainstream technology users are accustomed to, due to the unique operating and regulatory requirements around election infrastructure. Unlike an Internet-connected personal computer at one's home, for example, one cannot simply modify voting equipment merely by clicking a button based on new software made available by the manufacturer, online over a network. In other words, for voting systems, there is *nothing equivalent* to familiar messages which might appear on your device screen like this: "*Updates are available. Would you like to install the new version 12.5? Click Yes or No.*"

The main reasons that voting system update requirements are *very* different from mainstream consumer digital technology are:

1. All updated voting system software *must* go through federal and/or state approval processes before being released and installed; and
2. Because voting components are typically (but not always) "air gapped" (meaning that they are not connected to the Internet or other networks), changing their software usually requires physical labor in a warehouse, for example, such as inserting an external media (i.e., USB stick or DVD), or replacing individual memory cards in each voting device. That takes time and money, and is subject to human error.

Let's look at each of these challenges more closely.

3.1 Voting System Approval and Certification: Time-Consuming and Costly

Before voting system releases can be deployed in the U.S., approximately 40 states require the voting system configuration to be federally certified by the U.S. Election Assistance Commission[3] (EAC) before installation. This federal agency works with accredited third-party test labs, known as Voting System Test Laboratories (VSTLs), to ensure that each voting system release complies with the federal *Voluntary Voting System Guidelines*[4] (VVSG).

The federalcertification process poses significant challenges for rapid updates because the EAC certifies only *complete voting systems*, irrespective of how "incremental" or minor is the software change. Furthermore, although back-office election management system (EMS) computers and individual voting devices include a combination of operating system software (OSS) and proprietary voting system software on top of the OSS, they *cannot* be changed independently of each other, without resulting in a new voting system configuration or "version," which *must* be re-tested and re-certified.

These limitations mean that *none* of the following update procedure examples are possible under *current* federalcertification rules, without undergoing a comprehensive re-certification process:

---

[3] See: https://www.eac.gov/about-the-useac/

[4] See: https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/

- Operating system software on a back-office EMS computer or on a voting device *cannot* be changed or updated separately from the proprietary voting software; the OSS and the voting system software are bundled together and considered an integrated "package."
- Security "patches" or other minor updates *cannot* be applied to either operating systems or proprietary voting system software.
- Neither operating systems nor individual voting software applications can be changed without changing the "version number" of the overall voting system (e.g., if there is a small change in even *one* component of a voting system with many other parts, *the entire combination of components is considered a different "system version")*.

Given the need for manufacturers to achieve certification of the "total voting system," even a change in the operating system alone (e.g., updating from Microsoft Windows-7 to Windows-10) requires *significant* development and integration testing, followed by a long certification cycle.

Those factors also help to explain why vendors attempt to "hedge" their costs, with contract language about updates that reserves the vendors' right to impose additional charges for updates (i.e., charges above and beyond annual license and support fees). Neither development nor certification is free, and in the end, those costs flow down to election officials, either as hidden costs or explicit fees.

The net effect of all of these restrictions makes it impossible to develop and deploy software changes in a "modular" fashion, thereby ensuring that any updated voting system will almost certainly be "behind the times" — or even worse, *out-of-date* — the moment it reaches an election jurisdiction's warehouse. Even at a relatively fast pace, a federal certification for an updated system might require 3 to 6 months (and it could be much longer), and state certifications typically require at least 1 to 3 months; so, in the best case scenario, that's at least half a year (and perhaps closer to a year) before an update can be ready for implementation, not including the time it would take the manufacturer to develop and test the updated software – and that's *if* the manufacturer chooses to do so in the first place.

The bottom line is that the dynamic between voting system manufacturers and the federal EAC is broken: on the one hand, the EAC does *not compel* vendors to make timely technology updates (e.g., by prohibiting the use of outdated operating systems), nor does the federal certification program *facilitate* such updates. Given those two choices, and until something in the federalcertification program changes, commercial vendors are likely to continue choosing the easy way out by selling older certified technology, even if it has *not* caught up with the latest advancements.

3.2. Software Installation Process: Labor-Intensive with Potentially Marginal Gains

Assuming a software update were to be developed, certified, and made available to local election officials, there's *still* the question of actually getting it installed on all of the jurisdiction's PCs and voting devices. This requires physical activities such as replacing hard (disk) drives on EMS computers; labor-intensive staging of dozens, hundreds, or potentially even thousands of voting devices, so that USB sticks or other technology tools can be used to update firmware; and an intensive post-installation process of testing and formally "accepting" the updated devices (which is usually accomplished by running comprehensive diagnostics, or a mock election).

Furthermore, as noted above, due to the vague nature of contractual language around updates, which reserves wide discretion for vendors to do only what they want (including the possibility of charging for updates), local elections officials are left with much uncertainty:

- They may not be able to plan far in advance for when updates might be coming;
- Their flexibility is tightly constrained by immovable election cycles (which last several months at a time), during which changes to equipment cannot be made;
- They may not know how much the update process is going to cost;
- They may not have the budget to pay vendor fees associated with installation; and
- They may not have adequate personnel resources (in terms of either numbers or technical know-how) to install the updates themselves.

Finally, depending on the particular state in which the jurisdiction is located, there may be additional limitations on the nature of the work that can be done by the vendor, or by local jurisdictions. Some states (such as Colorado, for example) have an intensive "trusted build" process that is intended to protect the chain of custody of all voting system components:

1. First, the state receives the updated software directly from the appropriate testing lab;
2. Then the vendor must directly train authorized state technical staff to perform the software installation process; and
3. Finally, all installations must be performed (in each and every local jurisdiction) only by authorized state personnel — not by the vendor, and not by local officials.

As one can imagine, all of these uncertainties and restrictions have a direct impact on how local election officials *might* perceive the value or utility of installing any particular voting system software update. Indeed, in some cases, they might not bother. And even for those officials that do regularly update, because of the complexities of certification and installation, they will still be "last in line," with update software that is prematurely outdated.

> *The net result of these challenges is that much of the nation's voting infrastructure is likely to contain security vulnerabilities that were stamped out months or years ago by IT security teams in more mainstream organizations.*

So what, if anything, might improve things in the future?

4. What Needs to Change to Support More Predictable Voting System Updates?

Given the current limitations of vendor contracts, complex certification, and a unique operating environment, changes are necessary in order to provide voting system manufacturers with stronger incentives to upgrade their products and go through re-certification, and to provide local election officials with greater value in voting system updates (i.e., to make them less prematurely out-of-date). Below are OSET Institute recommendations for how federalcertification could be improved, and how local election officials can better arm themselves with critical information needed to enhance vendor accountability.

4.1 For Policy Makers: Re-Thinking Federal Certification

Coming up with new ways to support more flexible voting system updates requires policy makers and the EAC to re-visit some fundamental concepts and practices that make it almost impossible to rapidly update one or more components of a voting system. One of these has already been mentioned: namely, re-thinking the definition of "voting system."

Past federal certification campaigns have allowed only "total" system configurations, which essentially means that the EAC will only certify complete voting systems that include a comprehensive minimum set of end-to-end functions; vendors cannot simply make incremental changes in selected components and quickly deploy those updates. Recall, for example, that under current practices, if a voting system manufacturer wanted to update only the operating system software for only the back-office tabulation computers (which are especially important, since they count and report results), and nothing else, that change in the OSS for that one component would *still* result in an new "version number" *for the overall voting system*, and the modified voting system *as a whole* would *still* need to go through the long and costly federal certification process.

In contrast, there are alternative ways of thinking[5] of a "voting system" that could drive more flexibility in the federal certification program. For example, the ability for manufacturers to develop, test and seek certification for *individual portions of a voting system* (also known as *component-level certification*), rather than being required to submit only entire systems for certification, could introduce greater agility for vendors and local election officials alike.

In addition to those "carrots," the EAC could also consider additional "sticks," for example, in the form of new prohibitions on continued certification of voting systems whose operating systems are no longer supported by their manufacturer; in those instances, the vendors might be required to use updated/currently-supported operating systems as a prerequisite to (re)entering the certification process.

Finally, a heightened security environment might necessitate a new and larger role for institutions other than the U.S. Election Assistance Commission, with procedures that have been consciously crafted to be more flexible. For example, allowing the Department of Homeland Security (DHS) to oversee cybersecurity testing for voting systems, with a particular eye toward increased agility, could be a good first step in the right direction.

In sum, an evolving understanding of "voting systems," component-level certification, and re-thinking cybersecurity testing are essential because our national security depends on the agility that these programmatic changes can help to deliver. We hope that federal and state legislators will pay close attention to these evolutionary changes, because the cyber-threat landscape is rapidly changing[6], and in the future, the federal certification program must support rapid changes to voting technology.

---

[5] See: https://trustthevote.org/wp-content/uploads/2019/04/EAC_OSET-EPPTestimonySubmitted-10Apr19.pdf

[6] See: https://www.osetfoundation.org/research/2019/05/30/rethinktestcert

In addition to those changes in the regulatory environment, other changes could provide states, counties, and local election officials with other tools to hold vendors more accountable, so that the playing field is less unequal. As a final consideration, let's take a look at those.

4.2 For Election Officials: Education and Empowerment

Returning full-circle to the challenges that inspired this paper in the first place, it should now be clear just how complex the many factors are that impose limitations on how quickly voting system updates can be implemented.

In order for the overall security profile of our nation's voting infrastructure to be substantially improved, new incentives and sanctions will need to emerge in order to fill gaps in outdated software. As we have seen, however, common vendor practices and certification requirements play an outsized role in disrupting both the clarity and the pace with which potential software updates might be delivered.

Since certification practices are unlikely to change quickly, and because vendors are unlikely to willingly place additional obligations on themselves, the fact of the matter is that "moving the needle" to arrive at more predictable updates may rest in the hands of state and local election officials, who are uniquely positioned to increase vendor accountability during the contracting process. Vendors want to sell voting systems; they expend significant dollars for development, certification, operations, and marketing, and by the time an election jurisdiction announces an intent to award a particular vendor with a new sale, vendors are motivated to close the transaction with a mutually binding contract.

As this Briefing illustrates, the complex network of variables that impact voting system updates can be boiled down to just four (4) major elements that all procurement departments and election officials should become very familiar with; this is the initial "punch list" to guide their assessment of the playing field:

1. Initial Purchase. Review the purchase order, quote, or "bill of sale" closely. What hardware is included? What software is installed on the hardware? And what software licenses are already included for the first year?
2. Baseline Annual Fees. Review the "license and support" fee schedule carefully, to understand the costs that the customer will incur to continue using the hardware and software, year after year, over the term of the contract. License and support fees are typically listed separately from the initial hardware and software schedule.
3. Software Update Policies. In addition to reviewing the "license and support" *fee schedule*, carefully review any separate "*License and Support Agreements*," which are typically distinct from "*Master Agreements*" or "*General Terms*."

    3.1. Perform a word search for "*updates*" in all of these documents, and review the vendor's default boilerplate update policies. Accountability, transparency and predictability of potential software updates is likely to be enhanced by providing substitute language to replace the vendor's default software update policy.

4. Certification. state and local election officials should familiarize themselves with their state's policies around certification of voting system updates. The Secretary of State's office can provide information about timelines and policies for certification of voting systems.

With all of the above information as an initial baseline for negotiation, state and local election officials should now be in a position to collaboratively discuss more detailed questions with their preferred voting system vendor, *before* any contract is signed. The OSET Institute recommends discussing the following questions, among others:

- What types of updates are included through annual license and support payments, with no additional charges necessary?
  - Are security-only updates included as part of "software updates"? Who decides?
  - What types of updates might require additional, separate costs? Who bears those costs?
- If annual license and support payments provide the customer with "updates," does that include installation of updates, or is that a separate fee?
  - Are there any other additional fees associated with installation? Shipping? Consumables? Anything else?
- If any new software licenses are associated with the update, who will pay for them?
- Who is responsible for paying any third-party licenses that might be required to operate the updated system?
- How are updates installed?
  - By the vendor? The State? Counties?
  - What's included in "installation"? Does it include on-site service? Or is installation by the customer possible?
  - What is the customer "acceptance" process after the update is complete?
- Is there any way to predict and/or limit what software and security upgrades might cost (especially to facilitate budgeting)?
- Are there any circumstances in which the customer wishes the vendor to be obligated to provide an update?
  - For example, if a commodity off-the-shelf operating system or other major third-party component reaches "end of life" for support from the manufacturer, is the vendor obligated to do anything to update the system with a newer version? If so, how quickly must the vendor respond? (For example, "*Not later than 3 months after a commercial operating system manufacturer announces end of support for their product, voting system Vendor shall initiate a project planning process to collaborate with the county on a future anticipated update plan, subject to mutual agreement.*")

5. Conclusion

Given the fact that voting systems are part of our nation's critical democracy infrastructure, the outdated nature of much voting system software should concern all Americans. As this Briefing illustrates, election technology updates are a complex affair, and the limitations that exist today need to be improved. Currently, vendor behavior, vague contract terms, and disincentives

generated by a cumbersome regulatory process are preventing many of our nation's election officials from having voting technology that keeps pace with more mainstream advancements in a timely fashion.

In the current threat environment, outdated voting technology is an unacceptable security risk. This can and must change. As policymakers consider testing and certification programs for the future, they should *not* simply assume that past practices provide guideposts to the road that lies ahead; it will take careful thought and a concerted effort to create a more flexible path to regular, ongoing cybersecurity improvements in the future.

In the meantime, we say to state and local election officials, "*Now that you have more information, knowledge is power.*"

About the Author

Edward Perez is the *Global Director of Technology Development* for the OSET Institute. He focuses on election technology data standards, certification, audit, user-centered design and security-centric engineering practices. Edward also contributes to election law research, technology policy research, and government relations. He also is a principal liaison to the TrustTheVote Project elections officials stakeholder community. Mr. Perez earned his Master's degree from the University of California, Berkeley and his undergraduate degree from Georgetown University.

Prior to joining the OSET Institute, Edward directed product management for Hart InterCivic, one of the three major voting systems vendors in the U.S. Mr. Perez is a voting systems and election administration technology expert, with 15 years direct experience at Hart InterCivic where he applied his deep election administration knowledge to drive product development, voting technology design, federal and state certification, systems implementation, field service and support, and voter education initiatives.

Mr. Perez brings practical experience in all marketplace and technical requirements that structure the development and delivery of election technology to end-users in the United States, including voters, election staff, and polling place officials. Edward speaks regularly on these topics including most recently, the National Academies of Sciences, Engineering, and Medicine (NASEM), Committee on the Future of Voting, December 2017; National Conference of state Legislatures (NCSL), Future of Elections: Technology Policy and Funding Conference, June 2017. Mr. Perez is also co-inventor of U.S. patent US8985435B2 in the domain of voting technology assigned to Hart InterCivic, Inc.

About the OSET Institute

The Open Source Election Technology ("OSET") Institute is a 501(c)(3) tax-exempt nonpartisan, nonprofit election technology research corporation chartered with research, development, and education in election technology innovation. Federal Tax Charitable Corporation ID: 20-8743186; CA Charitable Trust ID: 0202910.

The Institute's flagship effort, the TrustTheVote™ Project is a "democracy software foundry" developing among other public technology, **Elect**OS™, a next generation higher integrity, lower cost, easier to use election administration and voting technology framework freely available for any election jurisdiction to adopt, and have professionally adapted and deployed. ElectOS and all open source election technology is being designed and engineered per the requirements and specifications of election officials, administrators, and operators through a Request For Comment (RFC) process.

As part of our research, development and education mission, from time to time, the Institute produces Briefings and other content to inform stakeholders, supporters, and the public about issues of election technology innovation and integrity.

Threats to our election administration technology infrastructure are inherently threats to our democracy

Supporter Acknowledgement

The OSET Institute, Inc. deeply appreciates Amazon Web Services ("AWS"), Automattic Corporation, the John S. and James L. Knight Foundation, the Democracy Fund, the Frost Foundation, the James H. Clarke Foundation, the Chris Kelly & Jennifer Carrico Family, the Barbara Coll Family, the Michael L. Henry Family, Matt Mullenweg, the Frank J. Santoro Family, the Peter F. Harter & Shelby Perkins Family, and the Alec Totic Family for their generous support of the OSET Institute's work to increase integrity, lower cost, and improve usability of election technology infrastructure in the U.S. and abroad.