Critical Democracy Infrastructure

Protecting American Elections in the Digital Age

Threats, Vulnerabilities, and Countermeasures as a National Security Agenda

2nd Edition | May 2020

OSET INSTITUTE

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.

The Institute's flagship effort, the TrustTheVote™ Project is developing **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

Foreword

By **William P. Crowell**
Former Deputy Director, National Security Agency; Partner, Alsop Louie Partners

In 2016 we witnessed a foreign state adversary launch successful attacks on our election processes and technology. The clear realization was that U.S. election infrastructure is a matter of national security. In 2017, the OSET Institute produced the first full treatment of the subject matter in the first version of this Briefing. The critical infrastructure designation by the former Administration was still new and drew partisan disagreement over what that meant. The new Administration allowed the designation to stand, which turned out to be beneficial for several reasons. Some wondered whether Congress should codify the designation. That hasn't happened and probably just as well. What remains clear is that election technology must be properly engineered, deployed, operated, and protected against attacks.

Russian, and now Chinese, Iranian, and North Korean state sponsored cyber-terror operations have been—as I predicted in 2017—refined to inflict enormous damage to not only the infrastructure, but the very trustworthiness of elections and their outcomes.

As a former Deputy Director of the National Security Agency, fortified by my continued engagement in breakthrough information security innovations ever since, I maintain the position I set forth in the first edition of this Briefing: In order to combat the threat of growing foreign attack capabilities, election technology must be redesigned using a security-centric engineering approach. This need to improve election security was true three years ago; it is even more imperative today.

I believe it is now undisputed that our election technology is obsolete, and relies on an untrusted dwindling supply chain of replacement parts. Polling places are mini data centers, and the fact that no Internet connectivity is involved is irrelevant to their security. Election administrators cannot be expected to counter increasingly capable cyber adversaries. Without a reset of the priorities for protecting election operations across the nation with better protocols, policies and platforms, our electoral process will be inflicted with increasing chaos, uncertainty, and upheaval. Proper protection is essential for trust in the operational results: accepted winners and losers, and the orderly transfer of power.

This second edition of the CDI Briefing synthesizes what we have learned in three years, and provides several recommendations. It offers a foundation of information on which to build more secure, lower cost, trustworthy election technology and processes. But, we're running out of time. The 2020 election is six months away at this writing, and I believe it will likely be the last national election that can be safely administered on the existing technology infrastructure and systems.

Unfortunately, continued polarization has made this topic of how to protect our election infrastructure nearly impossible. As I noted in 2017, this must change, and sadly it has not. My view is that the earlier we make the decision to reinvent the future election systems at some present cost, the better off we will be. Our adversaries may not have any partisan preference; they are opportunists. Therefore, we must pursue a patriotic approach. I believe this second edition of the OSET Institute CDI Briefing offers a discussion vehicle for securing this important aspect of our sovereignty in a nonpartisan way. I hope you agree.

Table of Contents

Foreword by William P. Crowell, *Former Deputy Director, National Security Agency* 5

Executive Summary 9

1. Increasing Risks and Critical Infrastructure 11
   - 1.1 The Mission 11
   - 1.2 Election Infrastructure Defined: Core Assets and Supporting Infrastructure 12
   - 1.3 Central Questions 13
   - 1.4 Briefing Outline 14

2. Basic Categories of Threats to Election Infrastructure 15
   - 2.1 Attack Targets: Distinguishing Election Infrastructure From the "Democracy Ecosystem" 15
   - 2.2 Basic Categories of Threats from Nation-State Adversaries 15
   - 2.3 Examples of Threats Applied to Election Infrastructure 17
   - 2.4 Examples of Threats Applied to the Democracy Ecosystem 19
   - 2.5 Summary 22

3. The Current State of Election Infrastructure Assets, Operations, and Threats 23
   - 3.1 Primary Election Infrastructure Assets 23
   - 3.2 The Current State of Risk to Election Infrastructure 24
   - 3.3 Synergies of Technical Risks 25
   - 3.4 Challenges of Protecting Election Infrastructure 26
   - 3.5 Steps taken by the EI Sector 27
   - 3.6 Summary 28

4. Findings and Recommendations 29
   - 4.1 Security Management of Voter Records Related Systems 29
   - 4.2 Technology Innovation for Voter Records-Related Systems 30
   - 4.3 Security Management of Voting Systems and Other Local Elections Infrastructure 32
   - 4.4 Paper Ballots and Audits 33
   - 4.5 Multi-factor Incident Response Planning and Public Relations Planning 34
   - 4.6 Technical Innovation to Resolve Current Voting System Platform Insecurity 34
   - 4.7 Hardware Supply Chain Risks 36
   - 4.8 U.S. Election Assistance Commission 37

Appendices 39
   - A. Overview of the U.S. Electoral Process 39
   - B. Election Infrastructure 43
   - C. Background on Critical Infrastructure 61

Citations 69

Glossary of Terms 75

Acknowledgements 81

Executive Summary

American democracy is now beset by nation-state adversaries who seek to weaken our country by undermining confidence in our democratic institutions, through attacks on or abuse of the essential infrastructure of the activities of democracy. Especially besieged is the democratic bedrock of free and fair elections—the very source of any government's legitimacy, and the basis for orderly transfer of political power. The current attacks target a broad range of entities including social media and other platforms for political discussion, the base of operations of political organizations and campaigns, and the process of voting.

All forms of attack on critical democracy infrastructure (CDI) should be of concern to all citizens of any democracy. However, CDI in the U.S. includes a particularly complex and vulnerable subset: the technology, people, and processes for administering elections and operating an election—especially the management of voter lists, and the casting and counting of ballots. This election infrastructure (EI) is critical to preserving sovereignty and protecting national security, and is designated as part of our nation's critical infrastructure (CI). Unlike the broader range of CDI, EI has bright-line boundaries: namely, the infrastructure of U.S. government election jurisdictions at state and local levels. In contrast to some other democracies, American EI is complex at nearly all levels, including the technological level—and is almost completely lacking in original design for robust defense against attacks by nation-state adversaries.

This paper focuses on election infrastructure, its definition and details; an assessment of current vulnerabilities and responses to them; and a set of findings for the issues most urgent to address in order to effect significant improvement in EI security, integrity, and trustworthiness. However, the broader vulnerabilities of CDI—including propaganda, disinformation, and attack on the infrastructures and processes of U.S. democracy—taken together with the specific vulnerabilities of EI can create a synergy that results in a more dangerous systemic weakness. That danger is also addressed in this report.

Mitigation of technologically enabled propaganda and digital disinformation campaigns present frustratingly thorny problems. By contrast, sound solutions already exist for several of the current weaknesses in EI technology and processes. Short-term responses and risk management have garnered considerable attention since the wake-up call of the 2016 election. But substantial risk reduction requires long-term planning and investment. This has begun, but only recently, and is still poorly understood by many of the stakeholders in election security and integrity. This report focuses on the most critical risk-reduction opportunities, those that would both strengthen intrinsic EI and also limit adversaries' opportunities for disinformation attacks—which, when coupled with effective attacks on today's highly vulnerable EI, become exponentially more powerful.

1. Increasing Risks and Critical Infrastructure

American democracy is now beset by nation-state adversaries who seek to weaken our country by undermining confidence in our democratic institutions, through attacks on or abuse of the essential infrastructure of the activities of democracy. Recently, these attacks have become increasingly focused in the cyber realm. According to Jeanette Manfra, (at this writing) Assistant Director for Cybersecurity at the Cybersecurity & Infrastructure Security Agency (CISA) in the Department of Homeland Security (DHS), "*Our adversaries have been developing and using advanced cyber capabilities to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democracy*."[1] It is likely that with time their capabilities will grow.

Especially besieged is the democratic bedrock of free and fair elections—the very source of any government's legitimacy, and the basis for orderly transfer of political power. The current attacks target a broad range of entities including social media and other platforms for political discussion, the base of operations of political organizations and campaigns, and the process of voting.

All forms of attack on "Critical Democracy Infrastructure" (CDI) should be of concern to all citizens of any democracy. However, CDI in the U.S. includes a particularly complex and vulnerable subset: the technology, people, and processes for administering elections and operating an election—especially the management of voter lists, and the casting and counting of ballots. This election infrastructure (EI) is critical to preserving sovereignty and protecting national security, and is designated as part of our nation's critical infrastructure (CI). In the words of CISA Assistant Director Jeanette Manfra: "ensuring the security of our electoral process is a vital national interest and one of our highest priorities at DHS."[2] Unlike the broader range of CDI, EI has bright-line boundaries: namely, the infrastructure of U.S. government election jurisdictions at state and local levels. In contrast to some other democracies, American EI is complex at nearly all levels, including the technological level—and is almost completely lacking in original design for robust defense against attacks by nation-state adversaries.

1.1 The Mission

United States elections are critical to our democracy, with a twofold mission:

1. To select political leadership and resolve questions of public interest (e.g., propositions or referenda), and
2. To ensure a timely and orderly transfer of power, which is in turn based on two critical election outcomes: the electorate's consensus belief in the legitimacy of election results, and concession of defeat by those not elected, based on the legitimate evidence of election results.

---

1 Jeanette Manfra, "Jeanette Manfra's Statement for the Record Senate Committee on Homeland Security and Government Affairs," *Senate Committee on Homeland Security and Government Affairs*, April 24, 2018, www.hsgac.senate.gov/imo/media/doc/Testimony-Manfra-2018-04-24.pdf.

2 Ibid.

Consider the impact on national stability if there were a major election in which a candidate did not concede, the public was not patient, and the massive echo chamber of social media (in infancy in 2000) amplified both real and spurious concerns and incidents, enabling organized unrest. Any lack of clarity on election outcomes can create dire threats not only to the orderly transfer of political power, but even to public safety. Basic consideration of a failed election process and consequent civil unrest indicates that the integrity of the election process is critical. At the national scale, threats to election integrity are threats to national security, particularly where nation-state actors may be engaging in operations to destabilize election processes or public trust of election results.[3] Where threats to elections involve EI, infrastructure for a critical function of our democracy, managing those threats and their risks is also a matter of homeland security.

Election infrastructure then, is indeed critical infrastructure. It is critical democracy infrastructure that is as important in its own way as critical power infrastructure, critical transportation infrastructure, and several other officially designated CI sectors that the Department of Homeland Security is tasked to provide assistance to as a result of Presidential Decision Directive 63 ("PDD-63") issued May 22nd, 1998 by then President Clinton.

In January of 2017 this resemblance between EI and CI became quite literal as then-Secretary of Homeland Security Jeh Johnson designated election infrastructure as critical infrastructure.[4] At the time this decision was met with significant criticism. Critics' concerns included worries about federal overreach into elections, a domain which the constitution grants to the states; the efficacy of critical infrastructure designation; and more. They are discussed in greater detail in Appendix C; however, the matter is now more or less settled. For better or for worse—and we at the OSET Institute are inclined to believe it is for better—election infrastructure *is* critical infrastructure.

1.2 Election Infrastructure Defined: Core Assets and Supporting Infrastructure

Bearing this designation in mind, it is important to understand what exactly makes up election infrastructure. EI can be thought of as two distinct parts: core assets that are integral to the casting and counting of ballots; and supporting infrastructure that, while not directly related to the casting and counting of ballots, is vital to the administration of elections.

Core EI is comprised of four parts: 1) voter registration databases (VRDBs), which are responsible for determining who is allowed to vote; 2) voting system components, which are responsible for receiving votes from the citizenry; 3) back-office machinery, which is primarily responsible for the tabulation and aggregation of votes; and 4) paper ballots and audits.

Beyond core EI is the supporting infrastructure. This refers to any other infrastructure that affects the casting and counting of votes, but is not handled by state election officials (SEOs) and election officials (EOs). For example, state websites that report election results or official communications from EOs to the public would be considered "supporting infrastructure."

---

[3] Max Bergmann and Carolyn Kenney. "War by Other Means." *Center for American Progress*, June 6, 2017, https://www.americanprogress.org/issues/security/reports/2017/06/06/433345/war-by-other-means/. Russia and other nation-state actors can use disinformation campaigns to sway the minds of individuals and destabilize America. While this has been done in the past, the advent of social media has increased its potency.

[4] Eric Fisher, "The Designation of Election Systems as Critical Infrastructure," *Congressional Research Service*, January 28, 2019, https://fas.org/sgp/crs/misc/IF10677.pdf.

Similarly, attacks on power grids or other supporting infrastructure that enables the use of core EI would also fall under this category.

Both core EI and supporting infrastructure are at threat from nation-state adversaries as a vulnerability in one might render futile strong security measures in another. For example, imagine an election in which the integrity of core EI remained strong, yet the state websites that report contest results were compromised and instead revealed results contrary to those reported by EOs across the country. It is likely that, despite high confidence in the integrity of the actual election results, Americans would struggle to understand which results were valid. Add into this the complex campaign dynamics associated with American politics and one can quickly see how trust in both the electoral process and those brought into power by it would waver considerably. False information, even once disproven, can be incredibly difficult to correct in the minds of the public.

The interplay between various components of EI make it clear that security in our elections relies on the security of the weakest link. As such, it is important that policymakers are holistic in their approach to election security.

1.3 Central Questions

However, even basic consideration of strengthening election infrastructure's security and resilience raises several questions central to the considerations of critical infrastructure. For instance:

1. What are the basic components of EI; that is, those assets referred to in the policy definition?
2. Which of those components are core technology for national security?
3. Of those core components, who is responsible for ensuring and delivering their fault tolerance in design and performance?
4. Who are the CI owners and operators, and what are their responsibilities?
5. How does the CI operator role fit within the role of elections organizations of many kinds?
6. How must DHS partner with election CI operators—as the agency has effectively partnered with CI operators in other sectors—to adapt to election administration, without running afoul of the reserved powers clause of the Constitution's Tenth Amendment that delegates the responsibility of administering federal, as well as state and local, elections to the states?
7. How is election administration and the election process itself affected by a CI designation, and in particular, what might be the costs, benefits, and trade-offs?
8. How can election administration be improved regardless of a CI designation? What might be those costs, benefits, and trade-offs?

1.4 Briefing Outline

The balance of this Briefing covers the following:

- Section 2 provides background in several areas: the current state of election infrastructure operations; their risks and compensating factors; a brief overview of the electoral process; and the challenges of ensuring the integrity of that process.
- Section 3 provides a general outline and overview of the current state of EI, deferring to Appendix B several areas of supplementary detail. Even an overview may require some familiarity with the processes of conducting elections, so for those with less familiarity, Appendix A provides some background.
- Section 4 provides our findings and summarizes recommendations into 7 areas:
    1. Voter records-related short-term technical risk remediation;
    2. Voter records-related technical innovation;
    3. Local voting system-related short-term technical risk remediation;
    4. Paper ballots and audits;
    5. Multi-factor incident response planning;
    6. Local voting system-related technical innovation; and
    7. Hardware threats and supply chain integrity.

This is followed by an set of Appendices that discuss within the scope of this Briefing:

- The U.S. electoral process
- Election infrastructure
- Background on Critical Infrastructure

2. Basic Categories of Threats to Election Infrastructure

Threats to our election systems come in many forms. Each component of EI comes with a unique set of vulnerabilities exploitable by nation-state adversaries. These threats are not limited to core EI but rather extend to all parts of election infrastructure and even to parts of the broader democracy ecosystem.

This section focuses on the main ways that nation-state adversaries can attack our election infrastructure and highlight how these various avenues of attack possess synergies with each other that have the potential to form an even more pernicious threat than that of a single type of attack.

2.1 Attack Targets: Distinguishing Election Infrastructure From the "Democracy Ecosystem"

This briefing focuses almost exclusively on election infrastructure: the machines and platforms that provide for the administration of elections. However, the broader electoral system is made up of far more than just government-managed machines and processes. Thus, any discussion of electoral vulnerability would be negligent to omit acknowledgement of this broader apparatus by which elections are conducted —termed the "*democracy ecosystem*."

The democracy ecosystem refers to all the other facets of elections outside of EI that can impact the results of elections. This includes, but is not limited to, political campaigns, fundraising organizations, and media outlets. These groups have great influence among the public and compromising any one of them could sway the results of any given contest and sow disorder among the people.

In order to administer free and fair elections, it is vital that the integrity of these additional parts of the democracy ecosystem is maintained. For example, if one candidate cannot run his/her campaign properly because the campaign systems are constantly subjected to distributed denial of service (DDoS) attacks, the contest would hardly be fair, even if all EI were to operate perfectly. Similarly, distorting media coverage of elections could impact its results, whether it be by feeding false information to reporters or by preventing news outlets from operating.

However, the democracy ecosystem outside of election infrastructure is *not* "critical" infrastructure; and maintaining its integrity is far more difficult. These actors must maintain a high degree of independence from the government in order for the democratic system to operate properly. As such, ensuring the integrity of these assets and organizations is far more complicated.

2.2. Basic Categories of Threats from Nation-State Adversaries

There are three avenues of attack nation-state adversaries can pursue in order to disrupt US elections. These attacks may be brought to bear against EI or against the broader democracy ecosystem. The three avenues of attack are defined based on three (3) kinds of outcomes that adversaries might seek to aacomplish, based on the end goal of the attack:

1. Subversion - manipulation of assets to undetectably *falsify an election result*

2. Defamation - disinformation attacks with supporting operations, that dramatically *impact public confidence in the legitimacy of election results*
3. Disruption - attacks that *impede voters' ability to vote*

Subversion is the most commonly discussed form of an election attack, but by no means should it be the only one to protect against; any of these three methods can compromise an election. While defamation and disruption attacks target the electoral and political system writ large, subversion attacks aim to help a particular candidate (or candidates) win a contest. For subversion to work effectively an election must already be close, yet it is worth noting that a targeted attack on specific precincts in battleground swing-states could alter the result of an election with surprisingly few votes being changed.[5]

Subversion attacks are not limited merely to attacks against election infrastructure itself; adversaries can also target political campaigns or parties, with the goal of changing election results. However, as stated earlier, this would not fall under the purview of critical infrastructure but is considered in greater detail later.

Defamation offers an easier, and perhaps even more powerful route for adversaries. In most cases, other nation-states may not have a strong preference for which presidential candidate wins the election, but sowing political chaos across the country serves the interests of any American (democracy) adversary. In the context of EI this might take the form of attacks that manipulate votes in a clearly discernible way, or the removal of government outlets that report results.

However, these attacks can also strike at targets outside of EI. In fact, of all the three avenues of attack, defamation is likely the best suited for attacks against the broader democracy ecosystem. Attacking campaign websites or media outlets with the intent of showcasing vulnerabilities are low-cost attacks with the potential for a high return on their investment.

Disruption attacks are distinct from subversion and defamation attacks. They may impact the results of an election or public confidence; however, the goal of disruption attacks is to manipulate the ability of voters to participate in a contest. Manipulating voter registration systems or shutting down the operations of polling centers would serve to achieve the objectives of disruption attacks. As with both defamation and subversion attacks, disruption attacks can also be levied against targets outside of EI. This includes misleading voters about the voting process and making it more difficult for them to register to vote or get to polling locations.

Subversion attacks have higher costs and risks compared to defamation or disruption attacks, which have a different goal: to destabilize the election process and reduce the public credibility of the process and its results—in other words, a direct attack on the basic objective of an election: yielding consensus results that are perceived as legitimate, followed by an orderly transfer of power (or retention of current office-holders, as the case might be).

---

[5] Tim Meko, Denise Lu, Lazaro Gamio. "How Trump won the presidency with razor-thin margins in swing states," *The Washington Post*, November 11, 2016. https://www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins/. Due to the way the Electoral College works, margins of victory that appear large can result from only a small number of individual votes. A few thousand votes can carry with them a large amount of electoral votes and thus, an entire election.

While the advent of social media and improvements in information technology have rendered these avenues of attack more potent, they are not confined to the cyber realm. Subversion attacks date back to the first attempts of ballot box stuffing, and defamation attacks have been known throughout the history of democracy. There a plenty of well-documented attempts by Soviet agents to use defamation attacks against the United States during the Cold War.[6] Disruption attacks can even be found in domestic and foreign attempts at voter suppression.

Finally, it is worth noting that these avenues of attack possess certain synergies. Subversion attacks may beget successful disruption attacks as trust in the legitimacy of elections is shattered through the manipulation of votes. Likewise, successful disruption attacks have the potential to alter the result of an election similar to a subversion attack. A targeted disruption attack — perhaps along party, racial, or social lines — could reduce faith in the election system and thus in government. Similarly, a defamation attack that reduces faith in the electoral system could depress turnout, which would have similar results to both subversion and disruption attacks. This highlights how any serious approach to election security must be comprehensive. Vulnerabilities to one avenue of attack open up vulnerabilities to the rest.

2.3. Examples of Threats Applied to Election Infrastructure

Each type of threat operates in a unique fashion based on its distinct goals. In order to provide some clarity on these different avenues of attack, this section offers some examples of each type of attack as applied to EI.

Subversion

The classic example of a subversion attack involves manipulating tabulation machines (typically desktop computers), a part of core EI. This can be done in a variety of ways. While these machines *should* be air-gapped, meaning they have no connection (direct or indirect) to the Internet, this may not always be the case, as computers used for elections may also be used to run day-to-day services. A computer that has not been air-gapped is likely vulnerable to spear-phishing attack or watering hole attack by which adversaries could gain access to either accounts used on the computer or the computer itself.

However, even if a machine were properly air-gapped, foreign adversaries would only need to find a way to insert compromised media (such as a USB storage device) into the machine in order to manipulate that county's results. While an individual attempt may not succeed, if carried out across the country in enough counties some are bound to find their mark. The malware might switch every fiftieth or hundreth result to the preferred candidate. Such a small shift would likely go unnoticed in an unaudited system; yet, as explained earlier, in a swing state it could easily flip an election.

An additional example of a subversion attack directed towards core EI would be an attack on voting machinery itself. For example, such an attack might flip how machines record votes, so that even before they arrived at a tabulation device they already reported incorrect tallies. Another iteration of this type of attack would be to alter voting machines in such a way that

---

[6] Alexander Lovelace. "2016 wasn't the first time Russia tried to sway a US election." *Washington Examiner*. December 29, 2016. https://www.washingtonexaminer.com/2016-wasnt-the-first-time-russia-tried-to-sway-a-us-election. This article from the Washington Examiner overviews the history of Russian and Soviet interference in US elections.

voters were more likely to accidentally select the wrong candidate. In fact, some have alleged that this occurred in the 2018 midterm election.[7]

Subversion attacks could even take place in voter registration databases. Here, the distinction between subversion and disruption attacks can become blurry as the means are identical, however, it is the end goal of the attack that provides the difference. A subversion attack levied against a voter registration database might alter the voter registration information of specific demographics of voters in order to impede their ability to vote. While this information can usually be corrected, it takes time and can discourage individuals, especially those on tight schedules, from voting. If the targeted demographic tends to vote for a specific party or candidate, then their inability to vote can ultimately flip an election.

Defamation

Defamation attacks represent a broader category of threats than subversion. In fact, poorly executed subversion or disruption attacks can easily result in defamation attacks; thus the bar for successfully employing a defamation attack is lower.

Imagine a situation in which just a few precincts across the country had their tabulation results altered in a clearly discernible way — Republican heartland turned blue while Democratic strongholds flipping red by absurd margins. It would be clear to most Americans that something had gone awry, and in counties without auditable systems one lingering question would begin to fester: *what about the ones we didn't notice*? If a couple of precinct results could be altered so dramatically then it stands to reason that others could be altered to a lesser degree. If Americans cannot be sure of the integrity of election results, then it would be unreasonable to expect them to respect the legitimacy of their elected officials and the government that represents them. This could lead to political chaos or at least the weakening of government legitimacy and efficacy.

Even if the attempt to alter tallies failed, the damage may still be done. News of attempts by foreign adversaries to infect tabulation machines, voting machines, or other EI with malware could spark similar concerns about whether there were other attempts that went undetected. Perhaps the ensuing skepticism could contribute to diminished turnout in the upcoming election, throwing doubt over the legitimacy of that election. It is then quite possible, that even without altering a single vote, foreign adversaries could impugn the legitimacy of elections.

A perhaps even easier attack to execute would be to poke and prod at voter registration databases (VRDBs) in a clearly visible way. As reports of this spread, it might be enough to create the appearance of a compromised system and diminish public confidence in elections.

If adversaries were able to compromise voting machines themselves, they could easily employ defamation attacks. For example, they could make specific election machines flash inflammatory messages to make it clear that they had been compromised. Even saying "*This machine has been hacked*" could be enough to put fear and doubt into Americans throughout the country.

---

[7] Tom Richell, "Midterm elections: Voting machine automatically selects Republican candidate instead of Democrat in Indiana, video shows," *The Independent*, November 7, 2018, https://www.independent.co.uk/news/world/americas/us-politics/midterms-2018/midterms-elections-video-voting-machine-malfunction-indiana-democrat-republican-a8621101.html Reports during the 2018 midterm elections alleged that voting machines were selecting Republican candidates over Democratic candidates in Indiana.

Defamation attacks can also strike at supporting infrastructure. One particularly pernicious method is through the targeting of state websites and media that report election results. Foreign adversaries could thus distort the results reported to the public on election day and portray incorrect results. At its worst this might lead to concession speeches made by candidates who actually won their race. Even if it were to be quickly remedied it could create uncertainty about the election results and engender fear that further damage had been done. The mere existence of these attacks is often enough to undermine public confidence in the electoral system.

Disruption

The easiest way to envision a disruption attack levied against EI is through the manipulation of VRDBs. By manipulating VRDBs, either locally or remotely, a malicious actor could alter a voter's address, party affiliation, or other information to prevent them from voting in the upcoming election or primary. This could take the form of an absentee ballot never arriving or even an inability to vote at the polls. While these issues might eventually be remedied, they can result in voters becoming frustrated with the government and either changing the way they vote or not voting at all. As prospective voters are denied from voting at poll booths and struggle to determine the reasons for denial, the waiting time at the polls will increase, leading others who were not directly targeted to not vote. Such disruption, if targeted correctly, could change the result of an election the same way a subversion attack would, or, especially if amplified by a disinformation campaign, could create the perception that a specific demographic was being disenfranchised, leading to the same result as a defamation attack.

While less likely, disruption attacks could target other aspects of EI. An attack that disabled or rendered more difficult voting at certain precincts could prevent targeted demographics from voting. An example of this would be malware that shut down or modified voting machines so that they were unable to register votes. In fact, any attack that disabled normal voting processes would function as a disruption attack.

Other iterations of these attacks could target supporting infrastructure. For example, modifying information on state or local government websites so that prospective voters would be unable to locate their polling locations; or impersonating public officials on social media platforms to release false information about how and where to vote.

2.4. Examples of Threats Applied to the Democracy Ecosystem

These avenues of attack apply beyond merely the realm of election infrastructure to that of the democracy ecosystem. This primarily involves attacking political campaigns or media outlets. Indeed, in some cases it is much easier for adversaries to select targets outside of EI as they may be less secure and there is less consensus on how to deal with them. Although these attacks fall outside the purview of EI, CI, and are not the focus of this briefing, it is worth explaining what they might look like and noting that they are distinct from similar attacks against EI.

Subversion

Election results can be distorted through foreign interference without directly compromising EI. The easiest way to imagine this is through interference in the political campaign process. Whether this is done by releasing false information regarding candidates, releasing campaign information, or directly attacking campaigns in an effort to prevent them from carrying out their day to day activities, the end result is the same. A prominent example of this is the John Podesta

eMail hack during the 2016 Presidential campaign, by which Russian state-sponsored hackers obtained work-related eMail of then-presidential candidate Hillary Clinton's campaign chair.[8]

However, there are other ways to attack campaigns. For example, a foreign adversary might use a distributed denial of service (DDoS) attack against a campaign headquarters to prevent it from running its operations successfully. A spear-phishing attack could also accomplish a similar goal. Federal investigators alleged that Russia tried to redirect donations to Democratic candidates away from their intended destination.[9] This too would be subversion. Regardless of the method, impeding a campaign's ability to operate could seriously impact the results of an election.

Attacks need not even target campaigns or media outlets. Foreign adversaries can impact the results of elections by inflaming the passions of the electorate. Depending on how such an attack is carried out it can either increase the engagement of the side it purportedly supports by sharing and distributing content to inflame their political passions; or, it can do the opposite by creating a strawman radical that outrages those of different political dispositions. Russian Twitter accounts have already done just this.[10] Foreign news outlets can also publish false or misleading stories aimed at distorting the perception of American voters. These stories might later be picked up by domestic outlets mistakenly believing them to be reputable sources and legitimate stories. Some have alleged that Russia has been doing this for past elections.[11]

Defamation

Defamation attacks on the democracy ecosystem utilize similar methods to both subversion and disruption attacks. In fact, sometimes it is difficult to determine which type of threat an attack is as the impact changes based on whether an attack is discovered. Any of the previously mentioned subversion attacks, upon discovery, are liable to reduce public confidence in the legitimacy of an election. Indeed, state controlled news outlets, internet trolls, and other social media instruments can be used to exacerbate and inflame public perceptions regarding alleged or perceived attacks, potentially resulting in a loss of public faith in the election.

Perhaps one of the clearest examples of defamation attacks on the democracy ecosystem are attacks that merely showcase vulnerabilities. Whether the target is a political campaign,

---

8 Raphael Satter, "Inside story: How Russians hacked the Democrats' emails," *Associated Press*, November 4, 2017, https://www.apnews.com/dea73efc01594839957c3c9a6c962b8a Satter's article retells how Russian agents infiltrated John Podesta's emails during the 2016 US presidential election campaign.

9 Philip Bump, "Timeline: How Russian agents allegedly hacked the DNC and Clinton's campaign," *The Washington Post*, July 13, 2018, https://www.washingtonpost.com/news/politics/wp/2018/07/13/timeline-how-russian-agents-allegedly-hacked-the-dnc-and-clintons-campaign Bump's article offers another example of how subversion can be applied to the broader democracy ecosystem; in this case by redirecting political donations.

10 Gillian Cleary, "Twitterbots: Anatomy of a Propaganda Campaign," *Symantec,* June 5, 2019. https://www.symantec.com/blogs/threat-intelligence/twitterbots-propaganda-disinformation. Symantec's report reveals how Russian social media accounts generated false new stories and amplified their message within the most disaffected parts of the political spectrum, on both the left and right.

11 Craig Timberg, "Russian propaganda effort helped spread 'fake news' during election, experts say," *The Washington Post*, November 24, 2016, https://ww.washingtonpost.com/business/economy/russian-propaganda-effort-helped-spread-fake-news-during-election-experts-say/2016/11/24/793903b6-8a40-4ca9-b712-716af66098fe_story.html. Researchers from the *Washington Post* found that Russian state-owned media outlets, such as *Russia Today* and *Sputnik* published false stories that would eventually get picked up by local news agencies.

donation website, or media outlet, showing that these facets of the electoral system can be breached is enough the disturb the citizenry. Imagine, for example, an attack that temporarily took down a prominent campaign website and displayed a simple, inflammatory message. Even though the attack did not change anything meaningful, it would engender fear that these adversaries could impact elections if they wanted to. It would also lead many to believe that foreign powers were taking measures to illegally support one party over another. The story would immediately be picked up by media outlets and spread around the country. Many would wonder who the perpetrator was and would launch accusations at domestic political opponents and foreign adversaries alike. The result would be a partial loss of faith in the legitimacy of the election.

Another example of this kind of threat is political inflammation aimed at one or all sides. When aimed at one side, it is likely intended to swing the results of a contest towards a favored candidate; however, when targeting both sides equally it is likely intended instead to disrupt the election process itself. One well documented case of this is the Heart of Texas rally and corresponding counter rally. During the 2016 election cycle, Russian agents created a Facebook event protesting the "Islamification of Texas" outside an Islamic center in Houston. The Russians paid to have the event promoted. A separate Russian-linked account set up a counter-protest to "Save Islamic Knowledge." Hundreds attended the event on both sides; and while no violence occurred, insults were hurled and tensions rose.[12] The impacts of such an attack are clear. If the perpetrators are discovered, many Americans will naturally feel that the election is being manipulated. However, even if the perpetrators remain anonymous or are believed to be Americans, the attack can still reduce the legitimacy of an election. Imagine if violence had broken out during the rally, as the organizers encouraged. The use of violence in politics can turn voters away from democracy, the execution of which should be peaceful. Even without violence, the sight of a radicalized opposition can leave many disenchanted with the democratic process.

There is an additional, and subtler harm to these defamation attacks: "*the liar's dividend*." Once the public is aware that foreign adversaries are, or are capable of, interfering, it becomes both easy and effective to dismiss opponents as trolls or bots rather than legitimate dissenters. Political discourse can be shut down on the assumption that it is illegitimate. Those who lose at the ballot box could claim to their supporters that their loss was at the hands of foreign interference rather than American voters. It suddenly becomes much easier to contest elections; or, even more pernicious, to refuse to give up power.

Disruption

Disruption attacks targeting the democracy ecosystem are somewhat more limited than the other avenues of attack. This is because the things that enable eligible citizens to vote are EI. Therefore, disruption operations outside of EI must either aim to mislead potential voters or impede efforts to increase voter turnout.

The former type of attack would generally be one aimed at misleading voters about when, how, or where to vote. A prominent example of this is the text-to-vote disinformation campaign.

---

[12] Natasha Bertrand, "Russia organized 2 sides of a Texas protest and encouraged 'both sides to battle in the streets,'" *Business Insider*, November 1, 2017, https://www.businessinsider.com/russia-trolls-senate-intelligence-committee-hearing-2017-11.

Voters were informed via various social media sources that they could vote for their preferred candidate by text message.[13] While this does not prevent a voter from casting a legitimate ballot, it is likely that if a voter believes they can vote by text they will use only that method and forgo proper voting methods, resulting in their votes never being counted.

Conversely, foreign adversaries could accomplish the same goal by targeting and impeding the operations of the myriad of non-governmental organizations (NGOs) that help voters register to vote or provide information about how to vote. While this does not, strictly speaking, impede the ability of eligible citizens to vote, it does make it more difficult for them to access materials and information that would help them to vote. These NGOs include Headcount, Rock The Vote, Vote.org, VoteAmerica, Voter Participation Center, VotoLatino, and more. They do not make up a part of EI, yet they play an important role in the electoral process of our democracy.

2.5 Summary

Core election infrastructure (EI), supporting EI, and the broader democracy ecosystem are three umbrellas of America's election system. They are all under threat, and attacks on one hold the potential to spill over into the others. Serious thought must be put into improving the security of each, as the entire system can only be as strong as its weakest link. The remaining sections of this briefing focus on core EI: those systems integral to the administration of elections themselves.

[13] Alexa Corse and Dustin Volz, "No, You Can't Vote Via Text or Tweet," *The Wall Street Journal*, August 11, 2018, https://www.wsj.com/articles/no-you-cant-vote-via-text-or-tweet-1533985201. This source overviews attempts to persuade voters that they could vote by text or other forms of illegitimate voting in what is believed to be an attempt to suppress votes from specific demographics.

3. The Current State of Election Infrastructure Assets, Operations, and Threats

A complete review of the current state of EI would be complex and lengthy. This section provides a general outline and overview of the current state of EI, deferring to Appendix B several areas of supplementary detail. Even an overview may require some familiarity with the processes of conducting elections. For those with less familiarity, Appendix A provides some background.

The starting point for an assessment of EI is an understanding of who operates EI – in other words, like any other CI sector, who are the "CI operators?" For elections, the operators are thousands of local elections offices, and the state elections offices that support and oversee their activities.

3.1 Primary Election Infrastructure Assets

Considering only the EI that is managed by election officials, the high-level list of assets is summarized below, linking primary assets to IT systems related to them.

- **Voter records**, and the IT systems that manage them, including: voter registration databases; voter records management systems, and voter lists created by them for several purposes; paper poll books, electronic (digital) poll books, and the back-office systems that prepare and manage them; poll book records of which voters checked in to vote, and where; Internet-based voter check-in systems for a whole county or state.
- **Voter registration systems**, including Internet-connected online voter registration systems: networked computing and storage systems that automate the *processes* of voter registration, where election officials respond to voter requests (and other events) to decide whether to add a voter to a voter roll, change an existing voter record, or remove a voter from a voter roll; including systems that compare voter records to other records (e.g., deaths, felony convictions, etc.) to match and flag voter records as candidates for removal.
- **Election management systems** (EMSs) used by election officials to manage pre-election data and processes (including ballot specification and proofing, ballot layout) and post-election report preparation.
- **Voting equipment** including DREs, ballot marking devices (BMDs), polling-place based devices for ballot counting, central systems for counting ballots; EMSs used to create "election programming" data for these machines; EMSs used to combine tallies from vote counting machines into vote totals and election results; removable media for shuttling data between these systems, and modems or network connections to transfer data.
- **Ballots**, ballot boxes, digital representation of ballots, removable media for storage and transport of such data, physical controls on them (e.g., tamper evident seals, multi-party custody documentation, etc.).
- **Cybersecurity assets** such as cryptographic keys used for data security; passwords or multi-factor authentication schemes for controlling access to any of the above IT systems or physical devices in a voting system.

- **The IT plant of a local elections office**, especially the parts that can have some connection to above assets; notably, workstations used for local election officials to access voter records systems; firewalls and other security mechanisms to control access to voting system components; the IT security infrastructure for authentication and access control that protects any of the above assets.
- **The IT plant of a state elections office**, both the office or "desktop" environment and the data-center; all the IT security mechanisms in the data center, most notably the security infrastructure for authentication and access control that regulates access by data center staff to election systems or data assets, and access to network and system security tools and systems.

3.2 The Current State of Risk to Election Infrastructure

As with the previous section, a complete assessment of threats and risks to EI would be complex, detailed, and a treatise of its own. This section provides an overview, consisting of a summary list of broad risk factors, each supplemented with details in the Appendices.

Hardware risks: Each current EI system has its own specific hardware platform. In every case, the components of the hardware platform were decided *without* reference to national security issues, and include hardware components delivered via an uncontrolled supply chain. Many EI systems pre-date the current recognition of significant hardware supply-chain risks. Most if not all EI vendors (as well as system integrators who support state-managed EI) lack the Supply Chain Risk Management (SCRM) skills and processes that are now standard for critical systems faced with hardware level risks. In fact, an Interos study of common voting machines found that 20% of components are purchased directly from Chinese-owned companies, while more come from Russia and China indirectly.[14]

System Tampering Risks: All current EI systems are subject to the wide range of typical cyber-risks of system infiltration, system and/or software tampering, data tampering/destruction/exfiltration, etc. Yet many EI systems were built *before* most of the current risks and threats were understood, and most of the EI operators lack the IT capability and cyber-skills to maintain a continuous monitoring and remediation program. These capability limits are *not* the fault of EI operators, but largely due to the fact that IT and cybersecurity funding for state and local EOs has lagged behind the recognition that these EOs are CI operators with election CI assets that are hardly defended compared to other CI sectors.

Software Tampering Risks: Of particular note among these risks and security gaps is the regulatory requirement that every voting system component, once certified, may *not* be modified from the certified software base. (Updates can be handled by deployment of a new version of a voting system component with an updated software base that has been re-certified; but modification in place, intentional or malicious, is forbidden.) Yet not all current voting system products provide local EOs with practical capability to examine each and every voting machine or other component, and determine whether its software remains in the pristine certified condition. These systems were simply not designed for validation in a hostile threat environment where nation state actors are among the threats to tampering with software.

---

[14] "Election Technology & the Global Supply Chain," *Interos*, https://cdn2.hubspot.net/hubfs/5812029/Interos%20-%20Election%20Security%20Paper.pdf

Appendix B provides details on the limits of current approaches to system control and validation of voting system components.)

Data Security Risks: Authenticity and integrity of critical data is an essential ingredient in election CI security. Data security techniques, such as digital signatures and other forms of applied cryptography, are available but are not effectively used. Among the data lacking effective protection are: the input data to every voting machine that describe the ballots to be presented and counted; vote tally data from ballot counting devices; voter records in voter databases; and more detailed in the Appendix B. In some cases, cryptography is used in an attempt to provide data authenticity, but actual practices (including poor key management, hard-coded keys, shared keys) often result in little real protection. In other cases, including voter registration databases, data protection is used instead, via user authentication and access controls that may be weakened by poor practices (such as single factor authentication; system or database administrative privileges subject to abuse to bypass access controls).

Limited Support for Evidence Based Elections: to remediate the technology risks to voting systems, the aspirational best practices include all paper ballot voting, machine counting, and manual risk-limiting audits (RLA) to detect and correct counting errors that would otherwise yield an incorrect election result. Yet at present, paperless voting machines are still in use (and in some cases still being purchased), while the majority of all-paper jurisdictions do not yet have the experience with RLA techniques to be able to actually deliver evidence that stated election results are correct election results. As a result, for most of the nation, there is little defense against concerns of election results tainted by technical issues of many kinds, including cyber-attack, unreliable hardware, software errors, and human error.

Fundamental Limits of Remediation: For the many kinds of IT management and cybersecurity risks described above, the current responses span a range of risk remediation approaches, compensating for the weakness of current EI with compensating controls in personnel security, physical security, procedural controls, increased use security monitoring technology, in many cases fortified by information sharing within the election CI sub-sector and with use of supporting services from DHS. Such remediation is performed with varying levels of resources, and varying degrees of compliance, by many EOs. However, most of the EI systems have fundamental cybersecurity weaknesses that date from their creation many years before the emergence of the current threat environment. Further, nationally uniform and high quality remediation programs, in every state and at every local level, are currently well beyond current funding and EO capability, and likely to remain so. An as-yet-untapped form of risk reduction is re-design of EI to reduce the currently wide attack surface, and to re-implement the most essential systems with cybersecurity designed in from the ground up. Current R&D in pursuit of this goal is promising, but years away from commercialization.

3.3 Synergies of Technical Risks

Taken together, several of these sources of technical risk have a synergistic effect. The above summary (with details in the Appendices) enumerates many omissions or defects of current EI technology that work together to create very significant technical risk. While not every item applies in equal measure in every state or locality, all jurisdictions have most or all of these risks in some significant measure, with the result that substantial synergies are possible to create significant security incidents.

The length of this list, the synergy between these issues, and the resulting high risk in the current threat environment, all combine to create our finding that remediation of cybersecurity risks of existing technology is *not* sufficient. While some remediation is required for best-efforts response to current threats, major cybersecurity vulnerabilities cannot be eliminated by remediation; remediation can only partly compensate, at significant cost. Dramatically reducing cybersecurity risk will require re-design of EI for cyber-defense, following by focus on essential security-critical EI assets, and re-design and re-implementation of them, for two essential principles: security-by-design to dramatically reduce the scope of threats; and enablement of election officials (EOs) to manage remaining risks with skills and tasks that are feasible (including fiscal feasibility) for state and local EO operations year-in, year-out.

3.4 Challenges of Protecting Election Infrastructure

Absent such dramatic risk reductions, and in addition to the specific technical risks described above, there are several other challenges to EI protection, many of which have a *common root cause*: election operations in the U.S. have grown organically, locally, and (with the transient exception of the impacts of HAVA) with largely state and local funding. Such funding was oriented toward operations rather than treating the technical infrastructure as critical infrastructure. With HAVA, the main goals for election technology reform were speed, ease, and confidence of vote counts; accessibility of voting technology; speed of voting technology refresh; and a new mandate for states to centralize voter registration operations.

For the most part, critical security and integrity protections were *not* fundamental requirements, and were entirely subsidiary to the goal of quickly replacing punch card and lever type voting machines. More recently, with the disbursement of a relatively modest $380 million of HAVA funding, federal funding has been provided with enhanced cybersecurity as a goal.[15]

Despite this one-time assistance of Federal funding, state and locally operated EI still faces many challenges, beyond the specific technical threats. Even a complete overview of challenges would be lengthy; the Appendices provide supporting detail to this brief overview.

Long-Standing Technical Challenges: The long-standing challenges to voting systems stem from the sources of technical risks outlined above. The consequence is the necessity for local EOs to provide additional safeguards that compensate for the fundamental deficiencies of current voting technology. The net result is an increase in the complexity of compensating physical and procedural security on the cyber-physical assets of voting system components, together with many unmet needs for staffing and funding to perform these compensating protections.

Ever-Increasing Technical Challenges: The IT footprint, and hence the attack surface, of EI has been increasing, with new targets such as: online voter registration systems; election night reporting data transfer over vulnerable data networks to election management systems; electronic poll books (ePBs); Vote Center ePB systems with real-time connections over vulnerable networks, Internet-based ballot return (via web, eMail, or fax), and real-time remote voting systems based on public networks and blockchain technology.

---

[15] "H.R.1625 - Consolidated Appropriations Act, 2018," Congress.gov, accessed May 12, 2019, https://www.congress.gov/bill/115th-congress/house-bill/1625/text. The full text of the 2019 Consolidated Appropriations Act, also known as the Omnibus Bill.

Ever-Increasing Compensating Security Challenges: As more IT becomes part of EI, state and local EOs must add additional layers of compensating physical, personnel, and operational security measures. Further, in an increasingly hyper-partisan polarized political environment, some EOs face challenges not merely in implementing such controls, but also in proving that such controls and other best practices have been actually performed (and audited for compliance) rather than merely instituted on a best-efforts basis.

Regulatory and market factors also create some substantial structural challenges to increased protection of EI, though there are also some more recent compensating factors, as described in in the Appendices.

3.5 Steps taken by the EI Sector

In light of all these challenges, the election infrastructure sector has taken some important steps towards improving its security. These developments are strong signs of progress, but taken alone remain far from sufficient.

One such development is the creation of sector-specific information sharing. Perhaps most important among these is the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).[16] ISACs, or Information Sharing Analysis Centers are common amongst critical infrastructure sectors and enable CI operators to communicate amongst each other to implement best practices across the board. The EI- ISAC focuses on cybersecurity in election infrastructure and includes both public and private members. Most notably, the ISAC includes not only state and local election officials, but also voting system vendors and other election technology companies.

In addition to information sharing within the sector, election officials are also learning from the Department of Homeland Security (DHS). The Cybersecurity and Infrastructure Security Agency (CISA), an entire agency within DHS, conducts cybersecurity risk assessments for state and local election officials.[17] Because local officials are rarely able to afford adequate training in cybersecurity, CISA's program helps bridge the gap between the knowledge and preparedness election official have and what they need.

DHS is also assisting state and local elections systems by deploying, with their permission, over 100 Albert sensors across more than 40 states, reaching around 90% of registered voters.[18] Albert sensors are intrusion detection systems that allow election operators, or in this case DHS,

---

16 "Election Infrastructure ISAC," *Center for Internet Security*, accessed on January 16, 2020, https://www.cisecurity.org/ei-isac/. This is the home website of the EI-ISAC. It includes a mission statement as well as members list, which notably includes a number of election system vendors.

17 "Cybersecurity Assessment," *The Cybersecurity and Infrastructure Security Agency*, accessed on January 16, 2020, https://www.dhs.gov/cisa/cybersecurity-assessments. This page offers a breakdown of cybersecurity risk assessments offered by CISA.

18 "Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure." *Office of the Inspector General Department of Homeland Security*. February 28, 2019. https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-24-Feb19.pdf. This DHS report assesses the state of risk to election infrastructure. Among other things it mentions the deployment of 100 Albert sensors across 40 states.

to monitor for malicious activity.[19] These systems can be used to detect intrusions into state or locally managed EI, enabling election officials to better protect their integrity.

Finally, Congress appropriated $380 million of HAVA funds in 2019 (and proposed another $425 million in late 2019) in an effort to help states update their election infrastructure.[20] The bill reflects a growing consensus among policy makers that current election systems are out of date and that a combination of voter-verified paper ballots and risk limiting audits are key to improving election security in the short-term. The EAC quickly dispersed the money amongst the states and they were able to start updating their voting and registration systems as well as begin implementing post-election audits. However, both state election officials and CISA Director Chris Krebs have noted that the funds are insufficient for some states and a one-time influx of cash will not resolve the evolving threats to election security.[21]

3.6 Summary

In this section, we surveyed the present state of EI security, with overviews of various kinds of critical EI assets, the current state of election operations using those assets, the current state of risks to them, the sources of those risks, and current activities to mitigate the risk as election technology progresses.

Based on this overview and supporting Appendix details, we can now address the scope for improvement from the current situation in the next section.

---

19 "Albert Network Monitoring," *Center for Internet Security*, accessed on January 16, 2020, https://www.cisecurity.org/services/albert-network-monitoring. In this page the *Center for Internet Security*, the creator of Albert sensors, explains the sensors' purpose and how they function.

20 H.R.1625 - Consolidated Appropriations Act, 2018," Congress.gov, accessed May 12, 2019, https://www.congress.gov/bill/115th-congress/house-bill/1625/text. The full text of the 2019 Consolidated Appropriations Act, also known as the Omnibus Bill.

21 Derek Johnson, "Officials push for more election security dollars," *FCW*, July 24, 2018, https://fcw.com/articles/2018/07/24/election-security-funding-ogr.aspx. Johnson quotes Chris Krebs as saying that election systems need to be updated across the board, and agreeing that on-going funding will be necessary.

4. Findings and Recommendations

Election infrastructure is now recognized as critical infrastructure—a result of the Department of Homeland Security's official designation in 2017[22] (see Appendix C). This has resulted in federal legislative activity (to fund state's election cybersecurity efforts), national security doctrine[23] that recognized past and ongoing adversarial attacks (including 2016 cyber-attacks on voter registration systems), and DHS priorities stated to Congress that emphasize election security.[24]

At the highest policy levels, policymakers and experts recognize the security of EI as critical to the legitimacy of elections, and to the stability of American democracy and government. However, there is a varying level of consensus about specific kinds of election CI technical assets, the cyber security threats to them, practical short term risk mitigation, and the limits of such mitigation. Our findings and recommendations below are based on the assessment of the main body of this document, a larger amount of appendix material, and the sources and references that support our assessment.

Our findings also pertain primarily to core EI. As discussed in Section 2, core EI is only one facet of the broader democracy ecosystem, and there are important synergies between vulnerabilities in core EI and vulnerabilities in supporting infrastructure and beyond. Policymakers can and should implement security measures in core EI independent of more holistic reforms -- but doing so will be insufficient to protect the integrity of elections.

4.1 Security Management of Voter Records Related Systems

There is broad consensus — among past and currently serving election technologists, policy makers, the intelligence community, and cybersecurity experts — that state and locally operated voter registration systems and voter records management systems are a critical part of EI. Moreover, the same groups acknowledge that these systems have been, and continue to be, the target of nation-state adversaries. They were not designed for the current threat environment; and as a result, they will continue to be vulnerable to cyber-attacks.

Managing these vulnerabilities is the goal of short-term cyber risk reduction of current systems in their current situation. Several states have made progress in increasing security management efforts, with assistance from DHS, use of a cybersecurity framework from the National Institute of Standards and Technology (NIST), participation in EI-ISAC and other information-sharing forums, and in some cases independent professional cybersecurity assessments. However, there

---

22 "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," *Department of Homeland Security*, January 6, 2017, www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designationelection-infrastructure-critical. Here Jeh Johnson, then-Secretary of Homeland Security, officially announces the designation of election infrastructure as critical infrastructure.

23 Daniel R. Coats, "Worldwide Threat Assessment," *Office of the Director of National Intelligence*, January 29, 2019, pg 7, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf. The Director of National Intelligence's Worldwide Threat Assessment reports on international threats to the United States. On page seven it discusses vulnerabilities within voter registration and vote tallying systems.

24 Kirstjen Nielsen, "Written testimony of DHS Secretary Kirstjen Nielsen for a Senate Committee on Homeland Security and Governmental Affairs hearing titled 'Threats to the Homeland,'" *Department of Homeland Security*, October 10, 2018, https://www.dhs.gov/news/2018/10/10/written-testimony-dhs-secretary-kirstjen-nielsen-senate-committee-homeland-security.

is significant scope for sustaining and expanding existing security management practices, and linking them to incident response planning.

Recommendations

4.1.1 Continue existing security management practices, including: continued assistance from DHS, continuing implementation of IT security best practices as defined by DHS and others, perform continuing vulnerability assessment, and perform vulnerability mitigation where operationally and fiscally feasible.

4.1.2 Retain independent professional IT security service providers to identify major risk factors (which will vary between states based on IT practices and datacenter operations and technology) and develop an incident response plan for future incidents of apparent or actual cybersecurity incidents pertinent to voter registration systems; include public relations activities as part of the scope of planned incident responses.

4.1.3 Leverage these short-term assessment and remediation activities to begin the process of instituting a complete security management program for all IT systems related to VR management (if not already present), using resources including those noted above. Included in the scope should be documentation and testing of data recovery plans to be used to recover from security incidents that may include data tampering.

4.1.4 For states with online voter services registration or OVR, with such assistance determine whether the core voter database is in any way accessible to public-facing systems, and if so, plan and execute a redesign to shift to the proven practices of other states that have OVR systems that are limited in access to a read-only copy of VRs, and a segregated system for storing OVR requests for later processing.[25]

4.2. Technology Innovation for Voter Records-Related Systems

Ongoing security management practices and related responses to current vulnerabilities are necessary to mitigate risk, but are limited in scope. Eliminating inherent vulnerabilities will require investment and technological innovation as states move to next-generation VR systems that are designed for cybersecurity from the start, in the context of the current and evolving threat environment. Until those next-generation systems with a different architectural foundation are built and deployed, VR systems will continue to be vulnerable and at significant risk for cyber-attack.

Recommendations

4.2.1 State election officials, state IT staff, and other election technologists should start now to look ahead toward development of next-generation VR systems that must be designed for a high degree of resilience to nation-state adversaries, and a high degree of protection/detection/recovery from attempts to tamper with voter records.

---

[25] John Sebes and Cliff Wulfman, "Online Voter Registration Systems: Best Practices," *OSET Institute*, March 5, 2018, https://www.osetfoundation.org/research/2017/9/11/critical-democracy-infrastructure-yss33. More information on online voter registration best practices can be found in this *OSET Institute publication*.

4.2.2 Use RFIs and similar outreach processes to ensure broad participation among technologists and vendors to:

- Assess the use of several promising technologies that can serve as ingredients for next generation VR systems: distributed digital ledger technology (DLT) for data security; modern cryptographic key management to support DLT usage; hardware cryptography modules for key protection; multi-factor user authentication including crypto hardware tokens for controlled access to VR systems and data; and server hardware based on new/emerging security-enhanced processors. The OSET Institute is already participating in this kind of research and development. For instance:
    - Design and development in collaboration with Accenture Labs and DXC Technology of a digital ledger security prophylactic called Vanadium; the alpha version demonstrated in October 2019 to DHS/CISA.
    - Research and development of strong authentication and security administration services for government web applications.
- Develop new security-oriented VR system architectures based on a decomposition of current monolithic VR system architectures into a data-centric security core for VR data management, and separate less privileged components for each of a variety of typical read-only uses for voter list data.[26] Some organizations, such as Intel[27] and DARPA[28] have already begun work on technology that could be applied here. Again, the OSET Institute is engaged in such research and development, for instance:
    - Collaboration with Silicon Valley stealth semiconductor technology start-up on trusted boot with hardware attestation technology—essentially hardware cryptography modules fpr security-enhanced processors.
    - OSET Institute's CTO collaboration with the Institute's security engineering partner, Galois, on their work with DARPA on the SSITH project.

4.2.3 Develop plans for multi-stage procurement processes to avoid vendor lock-in and monolithic systems, by separately procuring architecture plans, detailed designs, core VR implementation, and separate implementation of each less privileged component.

---

[26] Sebes, John, and Cliff Wulfman. "Online Voter Registration Systems: Best Practices." OSET Institute. Accessed December 21, 2019. https://www.osetfoundation.org/research/2017/9/11/critical-democracy-infrastructure-yss33.

[27] Develop & Deliver More Secure Solutions," *Intel*, accessed on January 16, 2020, https://software.intel.com/en-us/sgx. Intel is working on developing what it has named the Software Guard Extensions (SGX). SGX defines private enclaves within a systems memory that are protected from external processes, including those of higher authority. Only the CPU itself can decrypt the software, and even then only for code and data running within the enclave. The model treats all code outside of the enclave as suspect. SGX has a number of applications outside of election security, but most relevant to this Briefing, it could provide a way for election systems to, at their foundations, improve security.

[28] Keith Rebello, "System Security Integration Through Hardware and Firmware," *DARPA*, https://www.darpa.mil/program/system-security-integration-through-hardware-and-firmware. DARPA's System Security Integration Through Hardware and Firmware (SSITH) program aim is to create a hardware security architecture to reduce potential software exploitation. The goal is to protect systems from privilege, permission, memory error, information leakage, and code injection exploitations.

4.3. Security Management of Voting Systems and Other Local Elections Infrastructure

As for locally operated vote tallying systems (the combination of election management systems and computing devices for casting and counting ballots), there is a similar but not as broad consensus about criticality and risk, compared to the consensus on voter records. DHS and the intelligence community have released fewer details about past nation-state cyber-activity targeting local election operations. While most if not all of the 50 state-level election operations that are involved in Federal elections have been able to benefit from both internal IT security assessments and cybersecurity assistance from DHS, many of the thousands of small local elections jurisdictions have not been able to perform broad risk assessment and remediation. Regrettably, many U.S. election officials attach little significance to the cybersecurity risks of current voting system products, including some that continue to use old or procure new paperless voting machines, and continue practices of Internet connection of election management systems.

Recommendations

4.3.1 Local EOs should make voluntary use of DHS cybersecurity services to assess and improve controls over all local IT systems involved in election administration and election management, starting with a complete review and inventory of any system that handles pre-election data, preparation of systems for ballot casting and counting and post-election tally data.

4.3.2 Local EOs should leverage these short-term assessment and remediation activities to begin the process of instituting or strengthening a complete security management program, starting with independent assessment of documentation (e.g., compliance documents, training materials, product administration guides) of the complete set of physical, personnel, and procedural controls intended to mitigate risks of tampering with any components of the voting system, or systems on which they depend.

4.3.3 Local EOs should assess the recommendations made by several organizations (e.g., DHS, Center for Internet Security) for applying IT security best practices to local election infrastructure, and determine which of them are feasible to adopt in the near term, either as an initial effort, or as an enhancement of security management already underway. Although the scope is broad, we judge that a few particular measures could have a particularly significant impact:

- Implement EMS computers as single-function devices, completely air gapped, and physically access controlled for very limited access to required operators only. For cases where EMSs are network-connected for election night results reporting, use a secondary copy of the EMS just for these functions, while retaining isolation of primary EMS computers for tabulation.
- Institute and maintain rigorous hygiene on use of removable devices, always using new devices for data exchange between systems, to avoid the risk that a previously used device may have been contaminated. Where feasible, perform data exchange using read-only optical media as a preferred method, or Secure Digital card media, but avoiding to the greatest extent possible the use of USB data storage devices.

- If permitted by state voting system certification regulations, perform a clean rebuild of EMS computers on wiped hardware, to eliminate the risk of contamination from network or removable devices in prior usage (which may predate the tenure of the current local EO).

4.3.4 Retain independent professional IT security service providers to identify major risk factors (which will vary between local EOs based on different local practices and procedures) and develop an incident response plan for future incidents of apparent or actual cybersecurity incidents pertinent to local systems, whether related to vote tallying or not. While hiring more IT support staff with cybersecurity experience would also be valuable, this task is urgent and smaller jurisdictions with less resources on hand can turn to contractors.

4.4 Paper Ballots and Audits

There is broad — but again not complete — consensus among election officials, technologists, and policy makers on the most effective short term response to the cybersecurity vulnerabilities of current voting system technology: use of all paper voting (including a mix of absentee, in-person, hand-marked, and machine-marked ballots) coupled with risk-limiting audit (RLA) practices that:

- Detect situations where there is a non-trivial possibility that voting system malfunction (whether from malicious sources, operator error, software bugs, or hardware unreliability) has led to an incorrect election result.
- Enable corrections to report the actually correct election results.

While we share the consensus view, its practical utility thus far has been small. A small number of local elections jurisdictions (perhaps 100-200 out of several thousand) have or are in the process of developing and following state-specific routinized RLA practices. By some estimates it may be as long as a decade before a large portion of localities will actually be able to use RLAs to detect and correct tabulation malfunction situations.[29] In the meantime, the majority of ballots cast in Federal elections — even in all paper jurisdictions — will still be subject to potentially undetected errors.

Recommendations

4.4.1 Accelerate adoption of hand-marked paper ballots as the main voting method, for the majority of voters who are able to hand-mark a ballot.

4.4.2 Stop the acquisition of new paperless voting machines and replace all remaining paperless voting machines (DREs) with modern ballot marking devices (BMDs); though there is technologist disagreement over the relative merits of various BMDs, all agree that they have far lower risks than paperless voting machines.

4.4.3 Accelerating the adoption of RLA methods across the country is a widely held aspirational goal, but policy makers must determine how that acceleration will be funded and mandated for all localities in Federal elections. Wide but still limited adoption has

[29] "Securing the Vote," *The National Academies of Science Engineering and Medicine*, 2018, https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy.

very little benefit; in any state with a narrow-margin Federal contest (for members of the House and Senate, and for presidential electors), a single non-participating locality can undermine the benefit of an RLA.

4.4.4 Given that nationwide RLA adoption is a process that has proven difficult to accelerate thus far, states can begin by studying the additional expenses required to move all systems to voter verified paper ballots, and to add routine RLA operations. Both the initial shift and the continuing expenses associated with all-paper voting and uniform local RLA practices and state oversight will require ongoing, sustainable funding.

4.4.5 Similarly, the Federal government should consider how to fund these state-level studies, accelerate the studies themselves, and ensure that the studies provide the full range of up-front and ongoing cost analysis that would enable Congress to assess with reasonable accuracy the nationwide costs of adoption and ongoing support of paper and audits in Federal elections.

4.4.6 Meanwhile, local EOs can re-evaluate the physical chain of custody in order to promote public transparency in the way ballots are handled. Explaining the physical control over various voting system components will increase trust in elections. In some cases this may not even require changing the current system but rather increasing transparency in the process.

4.5 Multi-factor Incident Response Planning and Public Relations Planning

For both state and local incident response planning, a broad range of potential adversarial attacks (or spurious claims of attacks) are relevant. Adversaries can utilize multiple avenues of attack — including actual cyber-attacks; disinformation about cyber-attacks; disruption; disinformation about disruption; propaganda and social media amplification of disinformation — and achieve results that are of high value to adversaries, but without manipulating voter records or vote totals themselves. Therefore, current standard recommendations on incident response planning, focusing on cybersecurity threat analysis, are necessary but not sufficient. Incident response planning must *also* incorporate assessment of all avenues of attack, not only the technical; and incident response plans must include public relations and communications plans that address *both* real cybersecurity incidents and other non-technical (or not solely technical) attacks.

Recommendations

4.5.1 Both state and local election officials must develop robust incident response plans that address all of the different avenues of attack upon EI, including blended attacks that combine multiple methods.

4.5.2 Incident response plans should include public relations and communications plans.

4.6 Technical Innovation to Resolve Current Voting System Platform Insecurity

Current voting systems' base technology has fundamental security vulnerabilities as a result of dependence on common hardware and platform software that was not designed for a variety of essential aspects of voting systems, which are:

- National-security-critical CI systems, operating in a modern threat environment with nation-state adversaries.
- CI systems operated by local election officials who are now CI operators, but in almost all cases lack the technical resources to provide commensurate cyber-defense and other CI security protection.
- Dedicated systems that are intended to be (but are not in practice) tamper-evident, so that non-technical election officials can easily identify systems that are no longer in their federal- or state-certified configuration.

Because current voting system products were not designed for the current threat environment, and lack the cyber-defense required for national security systems,[30] it is essentially impossible for each and every U.S. local elections organization — in thousands of localities with varying budget, resources, and capabilities — to operate and protect voting systems with cyber-defenses commensurate with CI requirements.

The fault is *not* with election officials, but rather with the root causes discussed in Section 3, briefly, that current voting system products are built on decades-old platform technology that was specifically designed to enable systems to be easily modified, rather than to meet the opposite requirement that voting systems be tamper-evident for both software and for critical data that drives the software. The results for consumer computing have been an indefinite arms race of security exploits and countermeasures to further modify systems in reaction to exploits; and this arms-race approach to cybersecurity that relies on frequent security "patches" is now common as well in current voting systems, which must always be behind in the race, as a result of delays created by the voting system certification regimes in place today at the Federal and state levels.

The recommendations in subsection 4.3 above address needs to partly compensate for various effects of these root causes, but *cannot* remove the fundamental vulnerabilities. For future voting systems to be free of the wide range of current vulnerabilities, they *must* be based on modern security-enhanced hardware and modern system architectures that rely on it. Fortunately, that technology exists, is being enhanced, and is becoming available for general use beyond current applications in intelligence community defense computing that require high-assurance, fixed-function embedded systems.

Finding that the existing election technology base is fundamentally inappropriate for critical systems, the core observation is that it *must* be replaced. Our recommendations are objectives and courses of action toward that replacement, starting with fortification of existing research and development (R&D) to pursue the goal of new voting system base technology and fielded systems built upon it; systems with a base that is specifically designed for the security requirements of national security systems, and — equally important — designed for feasible CI operation by U.S. EOs. However, here is the key and vital point:

---

[30] "Glossary: National security systems," *Computer Security Resource Center*, accessed on January 16, 2020, https://csrc.nist.gov/glossary/term/national-security-system#targetText=Any%20information%20system%20(including%20any%20telecommunications%20system)%20used%20or%20operated,national%20defense%20or%20foreign%20policy.This source offers a useful definition of national security systems.

Attaining such a future election technology base will require a course of action that builds on current R&D in this area, to rapidly redesign and reengineer the underlying technology base for voting systems in a componentized architecture for fixed-function components that are fault-tolerant to withstand digital compromise.

In the R&D community, such work is in progress,[31] but needs acceleration both towards commercialization, and in application to the type of simple embedded system that is exemplified by voting systems components.

In the election technology community, there is also work in progress by NIST, the Election Assistance Commission (EAC), the EAC's Technical Guidelines Development Committee (TGDC), and many volunteers, on new cybersecurity guidelines for future voting systems; however, this work is oriented to current voting system technology, not toward embedded system cybersecurity; and this work proceeds slowly with minimal staff and funding, and high reliance on volunteers. Current voting system certification relies on over a decade-old guidelines used by voting system test labs with little modern cybersecurity expertise, resulting in many certified systems that subsequently were found to have significant security vulnerabilities.

Recommendations

4.6.1 Policy makers and current funders of embedded system cybersecurity R&D (including but not limited to DARPA and the National Science Foundation (NSF)) should develop methods to expand the scope of such R&D to include voting-related embedded systems, and to accelerate existing work toward commercialization, not only for EI, but for every category of CI that includes embedded systems that are safety-critical and/or national-security-critical.

4.6.2 Policy makers and current funders of voting system security guidelines development should develop methods to accelerate the existing standards and guidelines work on voting system cybersecurity, but with a new focus: requirements for those individual voting system components that must meet the most stringent challenges in the current threat environment.

4.6.3 Policy makers and current funders of voting certification programs should explore alternative certification and accreditation methods that are focused specifically on embedded system cybersecurity (in contrast to the current voting system certification regime), building on the standards and methods of security-specific certification programs that have been proven effective for security-critical systems relied upon by defense and intelligence community organizations.

4.7 Hardware Supply Chain Risks

There is broad consensus within the intelligence community and national security organizations, as well as some in the EI sector, that hardware supply chains are vulnerable to exploitation by nation-state actors. Until these hardware concerns are addressed, election systems will remain highly vulnerable, for both voting systems and for voter registration and voter records management systems. The below recommendations apply to the voting system ecosystem of

[31] Keith Rebello, "System Security Integration Through Hardware and Firmware," *DARPA*, https://www.darpa.mil/program/system-security-integration-through-hardware-and-firmware.

customers (local EOs), product vendors, product support vendors, and downstream supply chain partners of product vendors. Application of the below recommendations to state-operated voter records systems may be more challenging, because there is no vendor per se, and multiple state government organizations and/or vendors may be involved in sourcing hardware to run these systems.

In both cases, however, the essential observation is the same: hardware vulnerabilities must be addressed in tandem with other concerns in order to improve cybersecurity of EI, because the benefits of other cybersecurity improvements can be essentially negated by hardware level attacks.

The greatest hurdle, however, is that it is unclear at present which organizations should be involved in carrying out some of these recommendations.

Recommendations

4.7.1 Identify applicable proven examples of hardware component supply chain risk management ("SCRM"), particularly for common computer components and common server components, that might provide a model for SCRM for voting systems products, or for hardware acquisition of VR systems.

4.7.2 Identify existing government organizations that have set up and/or that operate an SCRM program and/or a closed supply chain.

4.7.3 States should develop a certification and accreditation process for voting system vendors to attest to sources of materials, as part of their SCRM program; and similar processes for servers of VR systems.

4.7.4 States should develop guidelines for preservation of certification of hardware-modified voting systems only when the replacement hardware components come from an accredited supplier; and similar guidelines for controlled hardware upgrades for servers of VR systems; and similar guidelines for original equipment manufacturers.

4.7.5 Policy makers must consider how oversight of EI supply chain is to be accomplished. Most states have little or no experience in oversight of vendor SCRM programs, while Federal government organizations with that experience are typical part of defense or intelligence community organizations. It may be that a Federal agency must fill that role, with requisite regulatory authority to administer and manage the supply chain for EI, in this case, perhaps DHS/CISA.

4.8. U.S. Election Assistance Commission

The U.S. Election Assistance Commission (EAC) plays a vital role in assisting state and local election officials. In particular, federal certification testing and the EAC's *Voluntary Voting System Guidelines* (VVSG) offer EOs evidence that their voting systems comply with federal standards for voting technology.

However, the EAC has largely failed to keep pace with the fast-moving field of election security, resulting in the approval of voting machines that are fundamentally insecure. In 2016, the agency announced the beginning of a process to update the federal standards to VVSG "Version 2.0" (VVSG 2.0). Unfortunately, despite significant initial optimism, bureaucratic and

institutional barriers have slowed the process of updating the standards, and because VVSG 2.0 is likely years away from being adopted and fully implemented, it remains an open question whether VVSG 2.0 will achieve meaningful change.[32]

The EAC's greatest burden is its lack of self-awareness. Unable to exercise introspection, the organization has failed to adapt to rapid changes in its operating environment. The EAC remains tied to a certification standard developed for a different era, adhering to the letter of the law in a way that restricts its ability to set useful standards. The agency relies on hundreds of functional and prescriptive requirements that ultimately stifle innovation, resulting in designs that are often obsolete by the time they are created.

In order to keep pace with the rate of technological progress and development, the EAC must figure out a way to make its guidelines more agile and flexible.

Recommendations

4.8.1 The EAC should create a distinction between principles and guidelines, and requirements. Principles and guidelines should reflect policy outcomes such as having a system be "voter-verifiable" or "auditable.") They can also be slower moving, relying on votes by the body to update. Meanwhile, requirements should be more adaptable and face fewer bureaucratic barriers. Requirements refer to technical necessities of a machine that are subject to change with new innovation.

These changes would make it easier for the EAC to keep functioning properly even if it were to lack a quorum of commissioners (which has happened in the past), as commissioners would only need to vote on new guidelines – but not on every modification to functional requirements.

4.8.2 The EAC should also allow voting technology to go through component-specific testing. This means allowing specific parts of a voting system to be tested independently. This creates a greater incentive for innovation at the component level as the entire system would not need to re-enter certification before a single part can change.

[32] Edward Perez and Gregory Miller, "Reinventing the U.S. Election Assistance Commission," *OSET Institute*, December 2019, https://www.osetfoundation.org/research/2019/08/08/reinventingeac. Perez and Miller's piece covers a number of flaws and potential solutions in the current US EAC, expanding upon the findings and recommendations found in this briefing.

Appendices

Appendix A
Overview of the U.S. Electoral Process

Discussion of election infrastructure assets and threats depends in part on some familiarity with the processes of administering elections and conducting elections. For those with less familiarity, this Appendix offers an overview.

Roles and Responsibilities

American election administration is collectively performed by an elections organization for each state and territory—often part of the office of its secretary of state—in conjunction with 6,467 local elections organizations,[33] each a part of a county or township government. The Tenth Amendment of the U.S. Constitution implicitly delegates elections as a matter for states to conduct, with considerable latitude for state decisions about how to do so. Among each state's individual policies for elections are policies for how election operation and administration are delegated to local governments.

The most significant change to the minimal structure for elections was the Seventeenth Amendment to the Constitution, which removed the states' right to define their own method for electing U.S. senators (often as an election within the state legislature), and created a national mandate for senators to be popularly elected in every state.

The most recent significant structural change in federal election operations occurred in 2002, when Congress passed the Help America Vote Act ("HAVA"). Among other things, Congress mandated that each state implement, manage and administer a "uniform, official, centralized, interactive, computerized statewide voter registration list."[34] Previously, each state could make its own policy ranging from state level administration of voter registration, to purely local administration with no consolidated statewide voter list at all—and several points in between. HAVA also created the U.S. Election Assistance Commission (EAC); a federal testing and certification program for voting technology; and it appropriated approximately $4 billion for the EAC to disburse to the states for purposes of upgrading old voting technology.

In 2018, Congress provided an additional $380 million in HAVA funding for the U.S. Election Assistance Commission to disburse to states for 2 goals: replacing vulnerable and outdated voting systems, especially paperless voting machines; and making improvements in cybersecurity of state and local elections operations.[35] The EAC disbursed the money to the

---

33 "2018 Election Administration & Voting Survey," *Election Assistance Commission*, accessed January 16, 2020, https://www.eac.gov/research-and-data/election-administration-voting-survey. For the sake of accuracy, given there are a couple of different ways in which this is calculated, we opt for the EAC definition. In fact, the number ranges from 6,400 to 10,000 depending on how certain outlying jurisdictions are considered.

34 "Help America Vote Act" *Election Assistance Commission*, accessed on January 16, 2020, https://www.eac.gov/about/help-america-vote-act.

35 "H.R.1625 - Consolidated Appropriations Act, 2018," Congress.gov, accessed May 12, 2019, https://www.congress.gov/bill/115th-congress/house-bill/1625/text. The full text of the 2019 Consolidated Appropriations Act, also known as the Omnibus Bill.

states, which were able to start updating their voting systems as well as begin implementing post-election audits. However, both state election officials and DHS Undersecretary Krebs have noted that the funds are insufficient for some states and the additional influx of cash will not resolve the evolving threats to election security that were initially discovered during the 2016 Presidential Election .[36]

Other aspects of federal-state interplay on elections have stemmed from the Voter Rights Act of 1964 and subsequent related legislation and jurisprudence. In these matters, the federal government asserted the right to constrain or oversee election administration within a state (often with respect to voter list management, ballot composition, and access to the voting process including early voting). However, such oversight did not mandate any diminution in state and local level operational responsibilities for election administration.

Likewise, other federal involvement in elections has been regulatory—as with the Federal Election Commission (FEC), which regulates campaign finance—or advisory, as with the Election Assistance Commission, and more recently some states' voluntary acceptance of cybersecurity support from DHS. The FEC's campaign finance mandate has been a major focus of regulation and legislation, but again, these matters have had little or no effect on how states choose to divide elections operations responsibilities between the state and its localities.

Activities and Operations

In terms of elections operations—that is, administering the process of casting and counting ballots, as opposed to a variety of pre- and post-election administrative functions—localities are responsible for administering elections in every state. The degree to which each state offers funding or operations resources and support to its localities' election offices varies.

More broadly, the majority of election administration is composed of these parts, each with the participation of local or state election offices (EOs).

- **Registration**. Voter registration, where a state has responsibility for the overall system, but local EOs provide the critical function of reviewing voter registration requests (and related requests), to approve or deny them. Varying by state, local and state EOs perform other critical functions such as voter list maintenance, which includes removing ineligible voters.
- **Candidate Management**. Candidate management is the process of qualifying candidates for a specific contest, and overseeing the compliance process that is largely focused on campaign finance disclosures. State EOs perform this function for state and federal contests, while local EOs do this for local contests. There is also an analogous process for ballot questions, including, but not limited to, referenda.
- **Voter Rolls**. Local EOs prepare and print paper pollbooks, and configure ePBs, using voter list data extracted from the voter registration system.
- **Election Definition**. Election definition is the process of compiling the final list of all contests, candidates, and questions for a specific election in a specific jurisdiction. State EOs provide local EOs the master ballot specification for state and federal contests and questions. Local EOs, working in parallel with the state, conduct their own processes, and incorporate

[36] Derek Johnson, "Officials push for more election security dollars," FCW, accessed May 12, 2019, https://fcw.com/articles/2018/07/24/election-security-funding-ogr.aspx.

the information from the state, to create the master ballot specification for the local jurisdiction.

- **Ballot Preparation**. Local EO election management processes include election definition, the creation of ballot specifications for each individual ballot, layout and printing of paper ballots, layout of screen ballots, and preparation of election-specific configurations for each component of a voting system, such as direct-record election devices (DREs), ballot marking devices (BMDs), precinct-count optical scanners (PCOSs), or central count optical scanners (CCOSs).
- **Logistics Planning**. Local EOs perform a considerable amount of logistics to convey voting equipment from a storage facility to a testing facility (often the local EO headquarters), configure the equipment with data from an election management system (EMS), perform logic and accuracy testing, and other testing, prepare devices for use (including tamper-evident seals), and convey them to polling locations. Closely related, local EOs prepare and distribute a variety of materials to be used in polling places, including paper and ePBs.
- **Poll Worker Training**. Local EOs train poll workers, arrange for the use of polling places, and provide support for the operation of polling places.
- **Absentee Balloting**. Local EOs conduct the vote-by-mail process.
- **Tabulation**. Local EOs perform the tabulation process of counting the ballots, creating a data set of tallies that are then combined and tabulated to create vote totals for the local jurisdictions.
- **Canvass**. Canvass is the review and official certification of the election results. Local EOs canvass their local contests and questions for which the vote totals comprise an election result. Local EOs submit vote totals for state and federal elections to the state EO, which is responsible for combining vote totals and certifying the election results.
- **Post Election Audit**. Increasingly, EOs nationwide are implementing election auditing as a standrd practice and this is becoming a significant element of operations. A post-election audit verifies that the equipment and procedures used to count votes during an election worked properly, and that the election yielded the correct outcome. A post-election audits can lead to a recount if errors are detected. Audits, however are different than a recount as they are (or should be) conducted regardless of the margins in wins and losses. Recounts, by contrast are triggered by those margins; the triggers are set legislatively. These activities and operations are the major parts of the election operations process.

Development of a more complete lifecycle is an ongoing part of the National Institute of Standards and Technology's (NIST) election data standardization, which includes work in progress on creating a complete business process model for election operations. Even NIST's work product will be mainly a common denominator that omits many localities' or states' specific election activities. Nevertheless, the above overview provides enough background on the use of EI assets for an assessment of the current state of EI activities and operations in practice.

Appendix B
Election Infrastructure

B.1 Election Infrastructure Operators

The starting point for an assessment of EI is an understanding of who operates EI; in other words, like any other CI sector, who are the "CI operators?" For elections, the operators are thousands of local elections offices, and the state elections offices that support and oversee their activities. These are the organizations that operate the EI assets that if successfully attacked—or even successfully discredited regardless of actual attack—can have national consequences.

However, as U.S. state and local elections organizations have evolved since the 1998-issued PDD-63 (when the national CI planning began, and then became subsumed by DHS post-9/11), CI was not a common organizing principle. Election officials ("EOs") today, considering themselves as CI operators, may well be taken aback, much as some other local-level CI operators were 15 or so years ago, upon learning that they operated CI such as local utilities, transportation authorities, and first-responder facilities.

In addition to an elections office, the full scope of EI operation also includes elements that are often outsourced in a way that has a potential for loss of control by CI operators that would not be typical in other CI sectors. For example, EI physical assets, such as voting machines, require storage and transportation that is typically outsourced.

Especially for small local EOs, a portion of election management itself is outsourced to a voting system vendor or a third-party service provider. For example, a local EO might specify the contents of an election's ballots, but provide those to a service provider that creates the election-specific datasets that must be configured into each type of voting machine.

Furthermore, local EOs as CI operators may have a somewhat larger role than CI operators in other sectors, taking into account **a**) the full scope of election-related critical democracy infrastructure — not just the primary assets but also the people and processes for managing them, and **b**) the election-specific requirements for critical democracy infrastructure that include record-keeping for evidence that demonstrates compliance with laws, regulations, processes, and procedures — and sufficient to enable adversarial situations such as recount and litigation.

B.2 EI Asset Details

The following sections provide more complete accounting for the many different kinds of assets in some of the asset classes described in brief in Section 3.

B.2.A Voter Records Management and IT Infrastructure

There has been long-standing and well understood recognition of the importance of the accuracy of voter records and the propriety of operations including voter registration and list management in voter records databases (VRDBs). This recognition attests to a clear understanding of each of the following assets related to voter records:

- Voter records as critical data stored in VRDBs.
- VRDBs as infrastructure for storing VRs and making them accessible to other infrastructure.

- Voter records management systems that EOs use to manage voter registrations (VRs) via support of list management processes; for example, identifying those records that match records of people who have died, who have been released from prison as felons, or who can claim a right to vote outside the U.S. — among several reasons for VR record modifications that are not initiated by voters.
- Voter lists created from VRDBs for any of a variety of purposes, including records requests, support for periodic reporting such as the EAC's Election Administration and Voting Survey ("EAVS"), and most notably the preparation of pollbooks for an election.
- Systems that use voter lists to create paper pollbooks or to prepare election specific data for electronic pollbooks (ePBs).
- Systems that used voter lists to prepare electronic poll books.
- Pollbooks and ePBs, and the voter check-in data recorded in them.
- Internet-based multi-site voter check-in systems, and the voter check-in data recorded in them.
- Systems that acquire pollbook records for voter check-in (including data entry or data capture from paper pollbooks, and data offloading from ePBs).
- Systems that combine acquired pollbook records with VR data to record checked-in voters and that aid in the process of absentee and provisional ballot processing, to ensure that each voter has no more than one ballot counted.

All of these forms of data and systems that manage that data are EI in the form of critical cyber assets; these and the people and processes of voter records management comprise EI that has a central role in public trust in elections: the assurance that ballots are cast only by authorized voters, that only legitimate ballots are counted, and that the voter lists that help provide that assurance are based on accurate data that is managed in accordance with relevant state election law, regulations, and processes.

With increased public awareness that nation-state adversaries target voter records in cyber operations, there is (or should be) a higher standard of care in operating the systems that manage voter records data. Recently, some states have begun to fortify their voter records systems' professional IT operations, with voluntary acceptance of cybersecurity and critical infrastructure operational assistance offered by DHS.

B.2.B. Voter Registration Integration and Infrastructure

The second of two critical aspects of voter records management comprises additional kinds of information techology (IT) for voter records processing beyond the voter-records management processes described above. As voter-records management systems become more interconnected with other systems, the IT infrastructure becomes more complex, with more threats, and a greater attack surface. Two typical examples of integration serve to illustrate the challenges.

The majority of states now support online voter registration (OVR) with an Internet-connected OVR front-end that collects voter registration requests in a digital form, and stores them for later processing in the primary voter-records management system. OVR is a bit of a misnomer, however: properly described, OVR is a method for digital submission of the same voter

registration request that voters can submit by paper. Digital submission has many advantages, but does not change the basic voter registration process: citizens submit requests, and local EOs review these requests together with other records, to accept or reject each request – regardless of whether the request arrived digitally, or arrived on paper.

When a legacy voter-records management system is augmented with network connections and/or dataflow from the Internet, new Internet-based attack vectors can be created; one example is the 2016 cyber-attack on Illinois' voter database.

There are two challenges to VR integrity and security that result from OVR, one specific and one general. The more general challenge of OVR is simply that all internet-connected systems are vulnerable to cyber-attack from the global communities of cybercriminals and nation-state adversaries. Conventional cybersecurity operations must be applied to cyber-defense and recovery from successful attacks that in today's threat environment cannot be categorically prevented. However, because public confidence in these public systems is crucial, then cybersecurity operations (at a very high level of capability) are warranted — which is probably not typical in today's first generation OVR systems. Originally envisioned as a "Web form" analogous to a paper voter registration form, these systems were *not* developed with consideration for CI.

The specific challenge is separation; that is, the operation of a new (Web-based) OVR system for submitting requests, as separate from the legacy (back-office) system for reviewing requests and managing the actual VRs. The former, by definition, is an Internet-connected system, while the latter must continue to be a closed, tightly controlled system without general access from the Internet. Typical IT security technology and operations methods must be carefully used to control the back-office system so that threats to the OVR system are not threats to the actual VRs. Fortunately, this form of separation is not unusual in cyber-CI, and existing methods can be applied to meet this challenge.

The second of two examples of integration is the integration of voter-records management systems with other state-managed systems, including but not limited to a state motor-vehicles department, for National Voter Registration Act (NVRA) compliance. The NVRA requires that motor-vehicles departments (and others), enable a customer to choose to submit a voter-registration request that re-uses the personal information provided for the motor-vehicles (or other agency) transaction. In cases where the voter-registration request is transmitted digitally to the state's voter-records management systems, the connection between the systems becomes a new point of threat. Attack on or insider abuse of the motor-vehicles department's IT systems can be leveraged to attempt attack on the voter-records management system.

B.2.C. Locally Managed Election Infrastructure: Organizations and Assets

By contrast to state operations centered on voter records management and voter registration, the majority of local election operations are small organizations without a dedicated data center, professional IT organization, or dedicated funding for technical security or security operations management. Large or small, these town or township, municipal, or county elections organizations manage a variety of technical EI, and a corresponding variety of people, roles, and processes for managing each kind of asset.

For a single local EO, the technical EI and related physical EI often consists of a variety of assets, including, but not limited to, the notable assets common to many election operations:

1. Computer workstations and/or servers running voting system EMS application software for functions including: election definition, ballot layout, voting device preparation, tabulation management, and reporting.
2. Computer workstations and/or servers running non-voting system application software for functions such as candidate filing and campaign finance compliance, physical asset inventory management, and personnel management including election-time temporary workers and volunteers.
3. Voting system components that include high-speed scanners with software for central count optical scanning (CCOS) of paper ballots.
4. Similar lower-speed components for precinct count optical scanners (PCOS).
5. Voting system components, such as BMDs, that provide accessible voting.
6. Paper ballots.
7. Physical infrastructure for absentee/by-mail, and for receipt and access control after receipt.
8. DREs, including those to provide accessible voting.
9. Paper record accessories for DREs that create a voter-verified paper audit trail (VVPAT).
10. Removable digital storage media that contain vote tally data from PCOS and DREs.
11. Computers or tablets running software for an ePB, sometimes with separate peripherals for signature capture.
12. Paper pollbooks and the IT systems that produce them from data from a voter records management system, and that capture information recorded in pollbooks.
13. Tamper-evident, physical integrity seals applied to voting system components before use.
14. Tamper-evident, physical integrity seals applied to equipment, ballot boxes, and other election asset containers, both before polls open, and after polls close.
15. Poll worker worksheets for logging setup and teardown activity, recording the ballot reconciliation process, tamper-evident seal checks and application events, and other required logging or tracking activities as required by state election law, regulations, and local election practices.
16. Physical chain of custody records.
17. Local voter records management systems used for adjudicating absentee ballots and provisional ballots, among other purposes.

Each local EO operates a substantial but locally varying subset of the above and related EI assets. The level of complexity of the assets and the asset management processes is evident from the above “highlights” list.

These assets and processes play a role in elections at every level of government: federal, statewide, state-level (e.g., counties, townships, municipalities), and a host of local special

districts, and must be protected. Protection functions are applied to uphold the integrity of the process as a whole, but election operations are fundamentally a local matter, ordinarily conceived of as a county or township government function — not as a national security matter that is delegated locally. The resources and expertise applied to local EOs' operations are those generally conceived of as appropriate to local government operation, albeit an important and visible one.

And in the majority of locales, local EO services are a periodic, part-time function of an office that also provides local-level services such as deed recording and business licensing.

B.3 The Current State of Risk to Election Infrastructure

The following sections provide more complete accounting for the many different kinds of assets in some of the asset classes described in brief in Section B.2.C.

Core EI technical assets are many years behind current technology, and were not developed with protections against the current threat environment. All are subject to tampering and other threats based on physical access, theft, or abuse of insider privilege. There is ample evidence of the vulnerability of voting machines,[37] EMS, ePBs, and VR systems.

While the basis of physical and social attack vectors may be evident to those familiar with election processes, there are several aspects of the current technology platform that require a more detailed explanation for two reasons: an understanding of deficiencies of the current technology platform and recommended requirements for the next generation of election technology. The current deficiencies include problems with verifiability, validation, immutability, assurance, and other desirable properties of trustworthy voting systems that were not specifically required by HAVA (or other post-HAVA laws), and hence, are not part of current voting systems.

B.3.A. Sources of Technical Risks: Hardware

One fundamental source of technical risk to core EI cyber-assets is at the hardware level, via threats from untrustworthy hardware components sourced from an open supply chain with no controls or provenance on acquired components.

This risk is particularly notable for voting system components, certainly during the manufacturing process, but more notably for EO operator maintenance in the use of replacement parts over the system components' extended life cycle. This practice has increased over time, due to the effect of market forces on the vendors, and to the effect of EO's reduced capacity for capital expenditures.

Since the passage of HAVA, the number of voting system vendors in the U.S. has shrunk to three vendors who together serve nearly all (approximately 92%) of the U.S. market, including two vendors who support the products of other now-dissolved vendors. At the same time, the ability of U.S. election jurisdictions to pay for voting system products has shrunk as well, with HAVA

[37] Robert Schlesinger, "Hack the Vote: a reminder of how insecure our ballots can be," *U.S. News & World Report*, July 31, 2017, https://www.usnews.com/opinion/thomas-jefferson-street/articles/2017-07-31/hackersdemonstrate-how-vulnerable-voting-machines-are. Individuals and organizations have repeatedly demonstrated, on request, the vulnerability of voting machines to manipulation by compromising the machines themselves.

funds exhausted and many state legislatures unable (or unwilling) to appropriate funds for localities to replace aging-out voting system components.

One result of this ossified market is that the maintenance of existing voting system devices depends on obtaining replacement hardware components from the global market in which components are sourced from supply chains dominated by vendors in nations that in other contexts are considered threats to national security.

As a result, U.S. voting system products have a supply chain risk, defined by 48 CFR 239.7301 (2) of Title 48 of the Code of Federal Regulations:

> *"Supply chain risk means the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a national security system (as that term is defined at 44 U.S.C. 3542(b)) so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."*

Although some may deem the likelihood of attack via supply chain to be low, the vulnerabilities in voting systems are pervasive, broad, and deep. Fortunately, experience in military supply chain risk reduction can be applied quite feasibly to voting systems. For critical military and/or classified information processing systems, concerted efforts have yielded, for some critical national security systems, a significant reduction in supply chain risk by the creation and maintenance of a closed supply chain limited to trustworthy component providers either U.S. based or based in definitively non-adversarial nations such as the I5 nations.

While this approach can be challenging for national security systems that have complex or domain-specific hardware requirements, the same is definitely not the case for the critical devices of voting systems. These devices' required functionality is quite simple compared to, say, a heterogeneous remote sensing array as part of a Command, Control, Communications, Computers, and Intelligence ("C4I") system. By contrast, critical voting system devices' functionality can be supported entirely by hardware composed of components that are completely common in ordinary PCs and scanners. As a result, a trustworthy closed supply chain may be more feasible to set up and maintain for future voting systems, compared to more complex national security systems requiring supply chain risk reduction.

B.3.B. Sources of Technical Risks: System and Software Modification

The current generation of U.S. voting system technology is massively mismatched for the current threat environment of cyber operations by state-sponsored adversaries with advanced capabilities. The mismatch arises from a core defect, where the post-HAVA voting system products were based on ordinary 1990's PC technology, where the entire software base is modifiable, and every system is capable of running any new software consistent with the hardware, whether the new software (or modification of existing software) is legitimate or malicious. This two-edged sword is typical for commercial computing in which flexibility is prized, and the consequently required defensive security arms race is an acceptable cost for the flexibility. However, flexibility is antithetical to voting systems.

The fundamental risk is not merely generally vulnerable legacy computing platforms as the basis of both ballot casting/counting devices, and back-office election administration software. With this underlying technology base, voting system components have a well known range of

vulnerabilities of legacy PC technology stemming from their design as general-purpose platforms.[38] As a result, these systems are *unable* to protect themselves in the current threat environment.

Failure to Meet System Control Requirements

Actually, the fundamental risk stems from the very flexibility of the underlying platform. Every voting system used by a locality's EOs must be certified by their state, and may not be modified. Prior to each use, every system must be revalidated to ensure that it remains in the certified configuration. The ability for a system to be arbitrarily modified, while useful for PCs, is completely counterproductive in voting systems.

The risk is *not* limited to legacy systems. Even the most up-to-date general-purpose platforms are fundamentally inappropriate for ballot casting and counting devices and critical back-office components of voting systems. General purpose computing platforms have a fundamental requirement to be able to be patched, updated, have new applications added to them, have applications that update themselves, and so on. These are malleable systems *by design*, which accounts also for their vulnerability to run malicious software. By contrast, critical voting systems have a fundamental requirement to run exactly one set of software, to not be able to modify that software, and to not be able to run any other software. Voting system components' requirements are exactly the opposite of a general-purpose platform.

Yet, with this antithetical technology foundation, current voting systems are just as vulnerable to attack as the ordinary PC technology they are based on. Years of experience in commercial computing have shown that the *fundamental risk cannot be contained*, only mitigated in an ongoing arms race between adversaries, and defensive technology creators and asset owners attempting to use the latest defensive technology.

The basic system control requirements come directly from the federal and state regulations on voting systems. A local election office cannot use a voting system unless the state has certified it as fit for use, often based on the federal process of voting system testing and certification. Certified voting systems must not be modified or extended; that would amount to the use of an uncertified system. Any needed changes must be made to the base hardware or software, and the resulting modified base must be recertified. Then existing fielded systems can have the older certified software replaced by the newer certified software — which again must not be changed in the field.

Limited Support for Feasible Validation

Another closely related property of certified voting systems is validation: the ability for an EO to inspect each individual device and ensure that it consists of hardware and software in the certified configuration, with no modifications. Because voting machinery is based on general-purpose computing platforms, not all voting systems in the field support a validation process; while newer systems can be tested for compliance with VVSG requirements to support external validation of software, many EOs must take on faith that there have been no changes (accidental

[38] "Computer Security Resource Center National Vulnerability Database," National Institute of Standards and Technology, accessed August 22, 2017, http://bit.ly/NVDsearch. The same Windows operating systems used by American election systems have long lists of common vulnerabilities and exposures (CVEs) that have been documented over the years and are publicly accessible.

or malicious) to the voting system since its last use, and conduct pre-election testing to ensure that each device behaves like a device in the certified configuration.

EOs do have methods to attempt to work around the fundamental malleability of systems. For example, they can use techniques for rule-based "check summing"[39] of a selected subset of a computer's file system. These approaches for system integrity self-checking have essential limitations, from the original "tripwire" technology[40] to all modern derivatives for file integrity monitoring and intrusion detection.

First, years of experience have shown that these techniques are only as useful as the accuracy of the inputs.[41] Such inputs are complex and system-specific rules, file system subset definitions and checksum baselines. Any error or omission in these inputs can produce false negatives (failure to detect an attack) or false positives; the latter can be specifically harmful for public trust in election outcomes.

Secondly, these techniques also have the basic limitation of any software self-check technique: an adversary who has gained the ability to tamper with a target system can also tamper with the self-checking software to prevent detection of the primary tampering. As these techniques have been applied to current malleable voting system components, the effectiveness is limited to accidental modification, which can cause a certified voting system to operate from an uncertified software base—an important situation to detect. However, these techniques are powerless against malicious modification by advanced adversaries, who can modify the system's self-checking code to provide inaccurate reports.

As a result, today's limited approaches to meeting validation requirements are approaches that are also unsuited to the current environment. These systems were simply not designed for validation in a hostile threat environment.

Redesign not Remediation

The resulting vulnerabilities can be remediated to an extent with compensating personnel, procedural, and physical controls. To various degrees, and with varying success in compliance, EOs in the U.S. do use compensating measures. However, the root cause can only be addressed with fundamental changes to the underlying system design, including avoiding the use of general-purpose platforms.

Current voting systems were based on general purpose computing platforms as a matter of expediency for time to market in the early 2000s when HAVA made available billions in federal funding to replace older election technology suffering from defects such as hanging chads, and lack of accessibility support for voters with disabilities. There is no technology currently in use in voting systems to support the requirement for fielded voting system components that can be immutable and validated.

---

39 See: https://en.wikipedia.org/wiki/Checksum

40 See: https://en.wikipedia.org/wiki/Open_Source_Tripwire

41 Gene H. Kim and Eugene H. Spafford, "Experiences With Tripwire: Using Integrity Checkers for Intrusion Detection," *Computer Science Technical Report*, Department of Computer Science, Purdue University, 1994 http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=2114&context=cstech. This article published by Perdue University offers an example of why security protocols and other such techniques are constrained by the accuracy of the inputs.

However, there are ample examples of available technologies in use outside of elections, for systems that do meet similar requirements. Generations of aerospace, communications, and defense systems have been built with an expanding toolkit of technologies for fixed-function embedded or dedicated systems designed to operate in hostile environments. The lack of application of these techniques to voting system component design is not an indicator of inapplicability, but rather of a lack of market impetus to redesign election technology in a major departure from the early 20th century approach that was driven in large part by time-to-market, cost-of-goods-sold, market pricing, return-on-investment, and market share preservation considerations.

B.3.C. Sources of Technical Risks: Data Integrity for Information Assurance

Election Officials' (EOs) mission includes significant components of information assurance. EOs manage a process that yields critical information: the winners of a set of contests and questions in an election, together with all the supporting details like voter check-in records, precinct level vote tallies, residual vote records, and more.

The information assurance mission is to provide assurance that this information is derived entirely and only from the legitimate voting of authorized voters. This mission depends on underlying data that is at-risk both as stored, and in-transit. Integrity and authenticity measures are essential to protect the underlying data so that as it is received and used, it can be validated as being from a legitimate source, and not tampered with since creation at that source.

Both voting system and ePB technologies have requirements for data protection. Voting system components generate vote tally data from ballot casting and counting operations. These must be securely stored with proof of origin, and protected with tamper evidence.

The risks of modification of tally data clearly include the risk of a modification changing an election result. The same is true of the voter check-in records created by ePBs. Since this data is an important input to the absentee ballot process, tampering of ePB data could result in disenfranchisement or fraud. Disenfranchisement could result from rejecting a specific voter's legitimate absentee ballot based on a spurious voter check-in record for that voter. After a specific voter casts a ballot in-person, deletion of the ePB record could enable counting of an illegitimate absentee ballot.

Both voting systems and ePB systems have similar requirements for legitimacy of their input data. For a voting system component, tampered or illegitimate ballot data could result in voters created invalid ballots. For an ePB, tampered or illegitimate voter list data could result in admission of illegitimate voters, or barring of legitimate voters. In addition to such election subversion attacks, both attack vectors serve equally well or better for disruption attacks and defamation attacks.

As a result of these information assurance requirements, voting systems and ePB systems have fundamental requirements for validation of integrity and provenance of input data, as well as creation of output data for which other systems can validate integrity and provenance. For these information assurance requirements, voting systems and ePB systems have data security functional requirements that include:

- Cryptographic key generation, distribution, and backup;
- Key ignition and key protection in fielded voting system components;

- Use of keys for output data protection; and
- Use of keys for input data validation.

Current voting system and ePB technologies are not capable of performing high assurance operation of these critical data protection measures. Current ePB products run on commodity PC or tablet platforms, with application software that was not subject to uniform security requirements, security review, or certification.[42] Voting system products, though certified, have also been demonstrated to lack effective data security measures. Every independent source code review or red team test has uncovered deficiency in data security implementations (e.g., hardcoded or otherwise shared keys, rather than key distribution).

Finally, these current products, being based on general-purpose system platforms, are unable to protect key data and cryptographic functions from the full array of malware threats that have been demonstrated for these platforms.

As a result, future voting system and ePB technology must be designed and implemented specifically for high assurance operation to meet data security functional requirements, including those identified above.

B.3.D. Sources of Technical Risks: Limited Support for Evidence-Based Election Results

Verifiability is a basic requirement for the election results produced by a voting system. A voting system must produce not only vote totals, but must also produce evidence that those vote totals comprise a valid election result. Risk-limiting ballot audits are a best practice for cross-checking the work of ballot counting technology by comparing machine counts of a subset of ballots with human counts of those same ballots.

For evidence-based verifiability of a voting system's results, the cornerstone is the basis in durable paper ballots of record that support two basic forms of election results: 1) rapidly produced machine counts by devices that support ballot audits; and 2) human conducted ballot audits. There is no single point of trust because there is no sole reliance on either a) humans to produce rapid, accurate, demonstrably impartial vote counts; or b) machines to function flawlessly in terms of accuracy or reliability. Machines can produce results impartially, rapidly, and usually accurately, while humans cross-check the results to detect and correct inaccuracy.

For this cornerstone to be effective, a voting system must not only produce ballots, but also must support ballot audits with specific evidence-related functions. These include creation of cast vote records ("CVRs"), and the effective use of cryptography to demonstrate "data provenance" of these records. This specific evidence enables local EOs to effectively use ballot audit techniques that are much more feasible in terms of scope and cost than today's common and unnecessarily labor-intensive process of fixed-percentage ("X%") ballot audits, where "X" is specified by law or regulation (and where audits are possible and funded).

In order for audits to be demonstrably adequate to verify results, the scope of audits needs to be carefully chosen for a process that is both feasible and transparent. A voting system must retain a CVR for each ballot, to support the most effective and least effort ballot audit procedure: risk-

[42] ePB software is fundamentally vulnerable to tampering that could result in compromise of cryptographic key data. No security review demonstrated effective measures to counter these data integrity threats, or even to validate that security functions are properly implemented.

limiting audits, based on sound statistical principles, using minimum size ballot batches randomly selected with constraints.

Current voting technology has limited support for verifiability. These limits include:

1. Paperless DREs: Early attempts at accessibility in the polling place led to DREs, many still in use, that unnecessarily combine the functions of accessible ballot marking, and tabulation of voters' choices. This combination created several issues: no support for verifiability; risks to vote tally data stored only digitally; and unequal risks, because paper ballot voters' ballots are verifiable, while DRE users' votes are at greater risk. Although being phased out in many jurisdictions, paperless DREs are still used.
2. Limited Tally Data: Many currently used voting systems that do support a voter verified paper ballot nevertheless lack support for risk-limiting audits, because of lack of single ballot CVRs or other requirements for such audits. As a result, audit batches are limited to machine counts batches (such as an entire precinct) and hence create a trade-off between significantly increased personnel and costs vs. less statistical confidence in election results. This seemingly technical defect also pits confidence against limited resources for the local election offices that conduct audits.
3. Proprietary Data Formats: Even where CVRs are available, they are stored in proprietary data formats (rather than an open data standard format) that can impede public access to ballot audit records. Ultimately, a risk-limiting ballot audit process is only effective if independent watchdogs can view the evidence of an audit, and determine that it was performed adequately.
4. Lack of Data Security: As described above, many current voting systems lack effective data security measures. As a result, CVRs (if available) and tally data cannot be demonstrated to be the legitimate, un-tampered basis for verification of machine tallies.

Progress on all the above issues will be required to create the conditions for truly verifiable evidence-based elections, including: accelerated adoption of hand-marked paper ballots; phase-out of paperless DREs; adoption of BMDs to replace paperless DREs for accessible voting; support for CVRs; and development of a national standard common data format for CVRs. That all of these trends are currently underway are positive developments.

Yet all of these factors still require high-assurance voting system technology that can both provide required data security measures, and provide system-level protections against subversion that can undermine data security measures. Further, the administration of voting systems, including cryptographic key management, must be feasible for ordinary EOs to perform.

B.4 Challenges of Protecting Election Infrastructure

This section of Appendix B provides more supporting detail on the challenges for EI protection that are summarized in Section 3.4.

B.4.A. Challenges for Cyber-Assets

Challenges to cyber-assets fall into two categories:

1. Long-standing systemic challenges and

2. More recent challenges.

The long-standing challenges to voting systems stem from the sources of technical risks outlined above. The consequence is the necessity for local EOs to provide additional safeguards that compensate for the fundamental deficiencies of current voting technology. The net result is an increase in the complexity of physical and procedural security on the cyber-physical assets of voting systems components.

CI operators in other sectors have faced similar challenges in applying complex physical and procedural controls to compensate for weakness in critical systems, notably legacy industrial control systems and supervisory control and data acquisition ("SCADA") devices that were designed and deployed without any concern of an adversarial threat environment. With the formation of an election CI sector, and learning from other sectors, there is reason to expect these challenges to be met with a higher regard for criticality.

More recent challenges stem from recent changes in U.S. election practice and will require either or both increased cybersecurity efforts and procedural controls. In other words, the technical complexity of election technology continues to grow, even as the stakes for protection increase, while, hitherto, there has not been a corresponding increase in CI protection efforts.

A small selection of recent additions includes:

1. Online voter registration (OVR) systems, which create new vectors of attack on VRs databases, if the Internet-connected OVR servers are improperly isolated from the database systems that manage the VRs. There are recently documented nation-state actor cyber-operations targeted at OVR systems. As described above, there is significant scope for improvement via better use of typical government datacenter IT best practices. However, robust defense against nation-state actors may require use of cyber-defense skills that are not common in state IT organizations. Recent recognition of the criticality of these assets, and their vulnerability to nation-state adversaries, has resulted (perhaps with some fortification from the formal CI designation) in new efforts in cybersecurity, with some states voluntarily obtaining assistance from DHS.
2. Internet-based ballot return, which exposes "digital ballots" to the full range of Internet-based security threats, and likewise the Internet-connected IT systems that facilitate digital ballot return. These practices create fundamental challenges, given the current inability to completely secure Internet-connected transaction processes systems of all kinds. Continuing policy discussions include a focus on in-theater military staff and the benefit to them of digital ballot return in situations where physical ballot return may not occur in a timely manner, even with the use of digital blank ballot delivery. With the possibility of nation-state actors, advanced cyber defense expertise will be needed for a balanced analysis of costs, risks, and potential detriment and benefit of these digital ballots.
3. Electronic Pollbooks (ePBs or e-pollbooks), which comprise another recent addition to election technology. ePBs manage critical election data: lists of authorized voters and records of which voters have already cast a ballot. Manipulation of this data can both affect voters' access to their ballot, as well as enable fraud via blocking counting of legitimate absentee ballots or enabling counting of illegitimate absentee ballots. Yet this data is not rigorously protected in current ePB systems, because ePBs face the same

types of challenges as voting machine components that use commodity platforms and were not designed for the current threat environment.

4. Internet-based voter check-in systems, such as that pioneered in Colorado, which use public networks to connect polling-place check-in terminals to a central voter check-in management system. The challenges are essentially the same as for any Internet-connected system, but the current bar of protection may be slightly higher, due to control of both endpoints. But again, with nation-state threats, advanced cyberdefenses may not be present in state-level IT organizations.

B.4.B. Challenges with Physical Assets

Physical assets face many challenges, especially for EI assets managed by local elections organizations. In a nutshell, each local elections organization has quite a substantial logistics operation to move, test, manage, distribute, and protect a variety of physical assets, including, but not limited to, the many types of assets listed above in Section B.2.C as Locally Managed EI: Organizations and Assets, and involved in the local level activities and operations listed above.

These base logistical challenges are substantial not only in scope and extent, but also in the responsibility for clearly stated policies and procedures for physical security, and adequate training for all relevant staff, including contractors and volunteers. These base challenges are further magnified by the responsibility for meticulous records-keeping to demonstrate that the procedures were properly performed and evidence maintained.

In other words, not only do EOs have to properly perform a number of controls, but they also have to prove that they did so, with evidence that can withstand an adversarial challenge to the propriety of election operations or the legitimacy of election results.

Given the recent unfortunate change in American political discourse to include concern over the so-called possibility of election "rigging," the importance of these challenges may in some cases be larger than the typical local election office's assumptions based on previous election cycles.

CI operators in other sectors have faced similar challenges in standing up rigorous and evident protection of physical assets. With the formation of an election CI sector, and learning from other sectors, there is reason to expect these challenges to be met with a higher regard for criticality.

EAC and DHS are working together on an essential response to the CI challenge of elections: formation of sector-specific organizations. One significant advantage that the elections sector has over some other sectors in the formational phase is that elections already have strong institutions for collaboration, including the National Association of Secretaries of State (NASS), the National Association of State Election Directors (NASED), the International Association of Government Officials (iGO), and several states' associations of local EOs. As co-sector specific agencies, EAC and DHS have convened organizational workshops with these stakeholder organizations, and leaders from representative state and local elections offices. The combination of existing sector institutions and an existing possible sector-specific organization, or organizations, with expertise in elections promises the sector formation activities might proceed in a timely manner.

B.4.C. Challenges for Personnel

As with any operation with physical controls, personnel security is a central pillar of protection. In the few large local election jurisdictions that comprise perhaps a quarter or more of the voting population, a local election office may have the ability to rely largely on employees. As a result, such organizations may be able to leverage a large local government's capacity for background checks, fine-grained employee-based physical access controls (e.g., badge-based controls), and other bread-and-butter personnel security measures.

However, even a large elections organization still relies on service providers of physical services (transportation, storage) and personnel services (temporary clerical workers for peak times), as well as a large number of volunteer or slightly compensated poll-workers. Personnel security is essentially absent in these cases.

For the majority of the many small elections organizations in the 6,500- plus localities in the U.S., personnel security capability can be limited or entirely absent, while the organizations must depend more on outsourced IT service providers and services contracted to a voting system vendor. In very small locales, the choice of service providers may be limited. Elections organizations are then essentially dependent on the personnel security measures of their vendors and of their service providers.

B.4.D. Challenges from Regulatory and Market Factors

Mitigation of these risks is hindered by some overarching factors related to the voting system test and certification process.

- The definition of a "voting system," is notoriously vague, but the de facto definition is the entirety of a system sold by a vendor; this can include numerous components or feature sets that are not critical to the creation of a verifiable election result. As a result, the scope of the test and certification process can be unnecessarily broad.
- The certification process is oriented toward testing of an entire monolithic voting system configuration, consisting of several interrelated and interdependent components (e.g., EMS, ballot casting and counting devices). Recertification of an updated voting system product requires retesting and recertification of the entire product, even if the update affected only a small part of the product.

Because of these and related issues, the voting system recertification process is slow and expensive for vendors, creating unintended market disincentive to provide incremental releases to EOs based on their feedback and new requirements for security and other characteristics.

As a result, there are significant hurdles to innovation that could address the shortcomings described above. Vendors have little or no commercial incentive to innovate their products with respect to security and assurance issues that were described above, and which are not explicitly required by their customers. Other innovators may have an improved voting system component (e.g., a ballot scanner with features to specifically support risk-limiting audits) but that cannot be certified unless it is part of an entire voting system product.

Partly as a consequence of these market forces and regulatory constraints, the sources of technical risk have not been systematically addressed. When the HAVA was passed in 2002, policy makers were not focused on cyber threats to voting machines. Election system vendors

did not enter the market as vendors of national security systems, and many, if not most, are not equipped to become such vendors. Even if vendors were equipped to sell the level of security appropriate for a proper election system, they lack the economic inventive to engage in such a costly research and development process.

Many jurisdictions across the nation must replace their aging-out voting systems soon. However, the current options presented to them all lack adequate improvements. While they will certainly make voting systems more reliable and marginally more secure, they do not solve the fundamental problems of a modifiable system. If counties choose to acquire these systems, due to lack of a better option, it will be years, perhaps even over a decade, before they can afford to buy a different system that is not fundamentally insecure.

B.4.E. Compensating Factors for Current Risks

The current status of election technology also includes activities that can enable the sources of technical risk to be much more readily addressed.

Efforts of the U.S. Election Assistance Commission and the National Institute of Standards and Technology

The EAC, working in conjunction with NIST, is currently engaged in a years-long process of developing new standards and requirements for voting systems (VVSG 2.0). The standards and requirements are prerequisite to changing the voting system certification process, to mitigate the market and regulatory factors described above. EAC and NIST's work in tandem is focused on a recently developed set of "public working group" processes for developing of requirements and standards that are intended to better enable both election technology innovation and reform of the regulatory hurdles to adoption. In terms of EI assets, the EAC/NIST work is most focused on voting systems (with occasional information exchange about e-pollbooks and VRs technology). While well-intentioned, the process has been fitful. The work described below is proceeding, but with relatively few resources, and plenty of scope for acceleration.

Open Data Standards

An open data standard consists of a technical specification of a common data format ("CDF"), together with explanatory documentation and examples. A CDF helps with inter-operability and data exchange by defining a common "language" to systems to communicate effectively with one another.

A recent example is a CDF for election definitions and election results. Early adopters of the CDF use it by converting from a variety of legacy data formats to the CDF, and publishing the resulting dataset as raw election results for general consumption. Based on the standard CDF, a variety of data consumers (news organizations, data scientists, academics, and other researchers) use the CDF in tools to obtain and interpret the data, where a single tool serves this function for any number of standards-based sources.

In the EAC/NIST election standards development effort, NIST publishes CDF definition documentation as guideline documents. In order for the CDF to become a true open data standard, the EAC needs to add a design guideline that certified voting systems must support the data standards for interoperability.

Certification Reform

Open data standards provide the basis for innovation in the architecture and operational model of voting systems. Currently, certification is based on a model of a large, monolithic, complex, low assurance system. The most potentially transformative type of data interoperability is interoperability between voting system components. Component interoperation provides the basis for a single component to be certified, which would be a major departure from the current certification program. This departure would enable some technology providers to focus on what they do best (e.g., accessible voting device design; digital image processing software; or hardware integration), and would enable EOs to choose individual voting system components that meet their needs best.

As a result, there would be markedly lower barriers to delivery to EOs of critical democracy infrastructure technology with innovations that lack the defects leading to the many technical risk challenges outlined above.

New Voting System Guidelines

New voting system guidelines are another important aspect of EAC's work. New guidelines are needed for the component-based certification described above. Critically, new guidelines can also specify new requirements for voting technology that currently are not required, such as evidence-based tabulation, support for risk-limiting audits,[43] supporting component validation, preventing unauthorized modifications, proper use of cryptography for data provenance, and others described above.

Support for component certification would not be limited to data standards and new requirements. New guidelines could also define the functional requirements for each component, requiring that each certified component conform to the standard product definition, and requiring the test labs perform conformance testing. This approach would be a major improvement to the current model, where each vendor defines each component in its own way, requiring the test process to be entirely customized every time.

Current Efforts and Resources

All of the efforts described above are part of an ongoing set of projects and working groups that are comprised largely of volunteers, and coordinated by a small number of staff and contractors at EAC and NIST, who also have other duties. The total funded level of effort might be as little as 2.5 full-time-equivalent staff. While the contributions of many volunteers are required to perform the work, the volunteer nature of the teams means that work progresses at an irregular pace. Taking the common data formats work, which now has over half a dozen active subgroups, the overseeing EAC commissioner aimed for a calendar year for substantial completion; yet efforts are well into the fourth year, albeit with notable deliverables such as a national standard data format for election results. The work on new cybersecurity requirements for voting system began even more recently; notable progress has been made, but there is no complete project scope or timeline.

---

[43] Mark Lindeman and Philip B. Stark, "A Gentle Introduction to Risk-limiting Audits," IEEE Security and Privacy, March 16, 2012, http://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf. Risk-limiting audits, in the context of elections, are a method that EOs can employ to ensure that the results of an election are accurate.

At this time, the decade-plus old certification program cannot be significantly updated until new guidelines and requirements are complete and promulgated. If there are to be substantial improvements in voting system technology as certified by EAC and by states, and put into fielded use, then at least two missing factors are needed for acceleration. First, additional resources are needed both for project managing these efforts to a timeline for specific impact, and also to bolster the efforts of volunteers. Second, such additional leadership and participation needs to inject national security and CI protection principles into the process.

B.4.F. Specific Government Efforts to Meet the CI Challenge

The EAC and DHS are working together on an essential response to the CI challenge of elections: formation of sector-specific organizations that are described in Section 3 and are the topic of one of our major areas of findings and recommendations in Section 4.

As previously noted, one significant advantage that the elections sector has over some other sectors in the formational phase is that elections already have strong institutions for collaboration.

Appendix C provides a background on critical infrastructure, election infrastructure as critical infrastructure, and the designation.

Appendix C
Background on Critical Infrastructure

C.1 What is Critical Infrastructure?

Critical infrastructure (CI) significantly predates the current discussion over election infrastructure. President Clinton created the designation of CI in the 1998-issued PDD-63, but it gained new significance three years after the attacks of 9/11. It established certain sectors of society whose assets, systems, and networks, whether physical or virtual, were considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.[44]

Since the first national Critical Infrastructure Plan established in 1998,[45] CI has expanded to cover 16 sectors: 1) Chemical, 2) Commercial Facilities, 3) Communications, 4) Critical Manufacturing, 5) Dams, 6) Defense Industrial Base, 7) Emergency Services, 8) Energy, 9) Financial Services, 10) Food and Agriculture, 11) Government Facilities, 12) Healthcare and Public Health, 13) Information Technology, 14) Nuclear Reactors, Materials, and Waste, 15) Transportation Systems and 16) Water and Wastewater Systems.[46]

Within any sector, a "CI operator" is the organization that operates critical assets that, if compromised, whether by physical method or by "cyber" means (i.e., via computers, networks, and other information technology) could result in significant national impact. That impact is significant regardless of whether the harm is accidental or intentional.[47]

CI operators include public corporations, private corporations, public utilities, and government organizations ranging from federal (e.g., air traffic control) to locally operated utilities (e.g. locally-operated utility companies). In addition, several kinds of government organizations are designated as first responders in certain cases of CI incidents or outages.

CI operators are responsible for the operation of a critical asset. Assets can be critical for several reasons. One familiar reason is continuity: we expect the power grid and the global financial transaction processing systems to be "always on" and resilient to significant disruptions. Other

---

44 "Presidential Decision Directive 63," Clinton Digital Library, May 20, 1998, http://clinton.presidentiallibraries.us/items/show/12762

45 Ibid

46 "Presidential Policy Directive—Critical Infrastructure Security and Resilience (Presidential Policy Directive/PPD-21)," February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. This web page includes, among other information, a list of all the critical infrastructure sectors before election infrastructure was designated as critical infrastructure.

47 Throughout this Briefing, nuanced distinctions like this are called out because of an overarching requirement to support "uplift" of CI. By "uplift," we mean more than concrete demonstrative actions. Uplift also includes the incorporation of personnel attitude, mindset, and "modus operandi." In this case for example, the intent, whether nonfeasance or malfeasance, should not alter the approach, protocols, processes, or (best) practices in assessing, responding, and handling any incident impacting a CI asset. In other words, an accident that harms a CI asset should be treated no differently than a willful malicious attack on that asset. Indeed, this will be new thinking to election administrators now tasked as "CI operators" (in addition to their duties in managing an election). The notion of "not taking it seriously, it's simply one of those things" is no longer an acceptable attitude. Uniform application of practices becomes a CI operator's mindset, and even removes potential partisanship concerns by treating everything uniformly.

assets may not always be on, but are safety critical; serious harm could result from malfunctioning of control systems at hazardous materials factories or water treatment facilities. Other assets, such as dams and bridges, constitute direct threats to public safety if targeted by adversaries.

C.2 Election Infrastructure as Critical Infrastructure

In 2017, then-Secretary of Homeland Security Jeh Johnson designated election infrastructure as critical infrastructure.[48] He cited the importance of elections and the growing need for cybersecurity assistance as reasons for the designation, but the logic behind elections being part of critical infrastructure extends beyond Johnson's rationale.

EI consists of all the assets necessary to successfully administer and operate an election. Disruption of EI can lead to a failed election—one that lacks conceding losers, consensus winners, and legitimacy for the transfer of power—which alone could be a failure of a "national essential function," (NEF) but also could have spillover effects on national security and public safety.

In terms of formal definitions, EI meets the basic definition when considered in terms of the basic mission stated above. Again, according to DHS, critical infrastructure ("CI") is comprised of the: "assets, systems, and networks, whether physical or virtual, considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[49]

With that definition in mind, EI may be considered CI in a fundamental sense, explicitly linking election administration to specific branches of government that have the responsibility to "strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions,[50] and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators."[51]

C.3 Election Infrastructure vs. Other Critical Infrastructure

Although EI is different from types CI in that it is not "always on," such as power distribution or air-traffic control, EI is similar to other CI sectors. For example, EI shares a characteristic with

---

48 "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," *Department of Homeland Security*, January 6, 2017, www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designationelection-infrastructure-critical. Here Jeh Johnson, then-Secretary of Homeland Security, officially announces the designation of election infrastructure as critical infrastructure.

49 "What Is Critical Infrastructure?" *Department of Homeland Security*, July 12, 2017, www.dhs.gov/whatcritical-infrastructure.

50 "National Continuity Policy Implementation Plan," Homeland Security Council, August, 2007, https://emilms.fema.gov/IS0545/documents/NCPIP_August_2007_508_Compliant.pdf. On May 4, 2007, President George W. Bush issued "the National Continuity Policy, an updated, integrated approach to maintaining a comprehensive and effective continuity capability to ensure the preservation of our constitutional form of government and the continuing performance of National Essential Functions [NEFs] under all conditions." NEFs include "the eight functions the President and national leadership will focus on to lead and sustain the Nation during a catastrophic emergency."

51 Barack Obama, "Presidential Policy Directive — Critical Infrastructure Security and Resilience," The White House President Barack Obama, February 12, 2013, https://obamawhitehouse.archives.gov/the-pressoffice/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil .

another important CI sector: finance. In both sectors, a critical part of the mission is maintaining public confidence in the correct operation of the assets. If there is significant loss of public confidence—regardless of actual malfunction or the degree to which malfunction affects outcomes—the mission of U.S. elections may be in danger. For both kinds of "transactions"—election votes and financial payments—the underlying CI must be able to sustain public confidence that the transactions are performed legitimately and accurately. Unlike power utilities distribution or air traffic safety, adequate transaction fraud prevention and detection are key parts of the mission; even further, these protections must be demonstrably adequate. The public requires a basis for the belief that the protections for elections are performed diligently, not the mere assertion by responsible parties that protection is in place. To be sure, there are critical differences from finance, such as that ballots must be anonymous, and the transaction of counting a ballot cannot be reversed. But some parallels exist, because there is process defined by law, available to any citizen, consisting of personal actions that must be approved and recorded. (Indeed, by a quirk of history, EOs such as Clerk-Recorders are often also literally in the transaction-processing business as much as the NYSE or NASDAQ—being county EOs on the one hand, but also having responsibilities as recorders of real estate transactions.)

EI also has similarities to other CI sectors that have locally operated assets, or government-operated assets. After all, we might reasonably expect stock exchanges and financial services companies to be able to operate critical systems, both because of organizational capacity, and because of the organizations' own self-interest in continuity of operation and in public trust in the legitimacy of transactions. Likewise, government operated air traffic control is safety critical and funded to meet stringent continuity requirements.

But do we expect state and local governments to exercise similar responsibility? Yes. Elections organizations have a fiduciary responsibility that is as imperative as that of financial services, and on election days has as much continuity responsibility as air traffic control.

But could we reasonably expect these state and local governments to develop similar capabilities for CI operation? Yes. Some CI operators are local government organizations, and the same is true of many first responders whose infrastructure is critical for public service and safety. Local government organizations operate water services, bridges and tunnels, and other assets essential to public service and safety. As CI operations practices have developed and extended to multiple sectors, state and local government organizations have evolved to conduct CI operations. There is every reason to believe elections organizations can do so as well.

Administrative Intent

The administrative intent of designating EI as CI need not be significantly different from similar designations in other sectors, especially those sectors where some CI operators are state and/or local government organizations. Although designation may not be, strictly speaking, required for any benefit, the major benefits would include prioritization, voluntary assistance, and voluntary sharing.

The administrative intent of CI designation should be a major re-prioritization intended to have a positive effect particularly on local elections offices' ability to gain assistance and resources. At

present, election operations are rarely treated as a top priority with national implications.[52] One possible parallel example is the positive impact that CI designation had on local first responder organizations to upgrade equipment and test response processes.

Other benefits are largely those of voluntary assistance and participation in sector-specific activities such as Information Sharing and Analysis Centers (ISACs). Again, an instructive analogy may be local water board operations, classified post-9/11 as public safety critical, and a very broad-scale vector of attack for homeland adversaries. From the first impact of CI designation up to the present day, the fundamentals of local water and sanitation operations have changed little. There is no DHS role in the operation of local utilities. There is no national regulation for required standard water treatment processes. There has been assistance to local organizations in performing asset classification, risk analysis, cost-benefit analysis, and other typical risk management activities that local utilities typically lack expertise in – particularly with respect to cyber-assets.

Specifically, with respect to elections organizations, constraints on change are more powerful and explicit than any other CI sector, including: Article 1 Section 4 of the U.S. Constitution, Article 2 Section 1, and Amendments 12, 15, 17, 19, 23, 26.[53] Likewise, historically elections have been notably free of directive federal legislation, with literally a handful of federal acts in many decades, and a near absence of federal regulation. With the notable exception of the FEC's role for campaign finance, Congress has not provided rulemaking authority regarding elections to any federal agency.

Not only does a CI designation not change the federal government's limited regulatory powers over elections, designation also does not create any new powers. For elections, as in every other sector, and with each designation of a new sector, the federal role has been as outlined above. CI designation in no way enables the federal government to have any new direct operational role in election administration, the operation of elections, or indeed any role in local or state EOs.

C.4 Initial Concerns about Designation of Election Infrastructure Sub-Sector

When the Department of Homeland Security designated Election Infrastructure as a Critical Infrastructure sub-sector in 2017, there was initially controversy about the designation. Critics' concerns included worries about federal overreach into elections, a domain which the constitution grants to the states; the efficacy of critical infrastructure designation; and more. Since that time, the states and DHS has made great strides in their cooperative efforts, and the matter is now more or less settled.

Below is a summary of some of the most common concerns that were voiced years ago, at the time of the original designation.

---

[52] Many localities have been unsuccessful in seeking financial and other resources to improve election operations. A major exception has been innovation grants from EAC and DoD/FVAP, but the aggregate nationwide funding in a decade is perhaps a few million dollars.

[53] "The Constitution of the United States: A Transcription." National Archives, June 26, 2017. http://www.archives.gov/founding-docs/constitution-transcript The Constitution of the United States delegates the elections largely to the states and restricts the influence the federal government can have over them. Through multiple amendments it also dictates certain characteristics of elections.

C.4.A. Federal Influence in Elections

Perhaps foremost was the concern, as voiced by Georgia's then-Secretary of State Brian Kemp, about undue federal government influence or involvement in state and local election administration and operation.[54] However, it is important to note that any relationship between CI operators and DHS is voluntary. EOs can determine the scope and duration of their interactions with the DHS; the designation merely makes EI a priority for resources and assistance should an EO want them. Regarding Homeland Security, the actual history of DHS's role in other CI sectors does not suggest DHS intrusion, or potential thereof, into election operations.

Nevertheless, federal involvement in elections is conceivable. While primary authority over elections rests with the states constitutionally (i.e., the Tenth Amendment), the federal government does retain (little used) authority over elections for federal offices (i.e., Congress and the President), so reasonable legal experts can argue over what this could mean. Thus, we regard it as a fixed point for any effective federal role, by DHS or otherwise, with or without an official designation, that the existing administrative structure of U.S. elections be left unchanged and untouched.

C.4.B. The Scope of EI Designation

Initial lack of clarity on the scope of EI designation also created concerns,[55] but the subsector designation applies strictly to the EI operated by state and local elections organizations; it does not extend to the infrastructure of the many non-government organizations involved in the larger political process outside of administering elections. For example, as Christy McCormick, an EAC commissioner, rightly points out, issues such as "what happens on or to the e-mail systems of political parties or their committees, purported influence campaigns, and celebrations for one candidate or another, have no impact on the security and integrity of our election infrastructure."[56] Political parties and their e-mail may be a part of a broader *democracy ecosystem* but they are certainly not a part of EI. As EI sector formation activities have evolved, it is important to note that the scope of sector activity does not extend beyond government-operated EI.

C.4.C. Federal Regulation of Elections

Some have wondered whether the CI designation makes it politically expedient for the federal government to regulate elections for national security purposes.[57] However, an increase in political expediency, if present, would not change the fact that today, there is no part of the executive branch that has rule-making authority over elections, other than the FEC's oversight

---

54 Tim Starks. "DHS labels elections as 'critical infrastructure'". Politico, January 6, 2017, http://www.politico.com/story/2017/01/elections-critical-infrastructure-homeland-security-233304

55 "Securing Elections as Critical Infrastructure," National Association of Secretaries of State, accessed on August 17, 2017. http://www.nass.org/index.php/nass-initiatives/nass-cybersecurity-elections-critical-infrastructure/

56 Hans Spakovsky, "DHS' Election Power-Grab Raises Huge Questions and Red Flags," *The Heritage Foundation*, January 13, 2017. http://www.heritage.org/election-integrity/commentary/dhs-election-powergrab-raises-huge-questions-and-red-flags

57 Pam Fessler, "State And Local Officials Wary Of Federal Government's Election Security Efforts." National Public Radio, April 5, 2017, http://www.npr.org/2017/04/05/522732036/state-and-local-officials-waryof-federal-governments-election-security-efforts

of campaign finance. Any future increase in federal regulation would require Congressional legislation to grant some rule-making powers. To date, the existing designation seems to have had little if any impact on the desire of Congress to provide greater regulatory authority beyond that already granted to the FEC. Indeed, currently there remains on-going Congressional debate over funding for the U.S. Election Assistance Commission.[58]

C.4.D. Permanent Designation by Congressional Action

Some have also wondered whether Congress might legislate that elections be permanently classified as critical infrastructure, as H.R. 1562 sought to do in 2017.[59] It is unlikely that DHS's designation will affect Congress's views on critical infrastructure, but even if Congress were to create a permanent designation, it could never interfere with State's constitutional right to administer elections. The states have hundreds of years of experience running elections that the federal government lacks; there is no evidence that critical infrastructure designation is any attempt to limit or remove states from that role; indeed, all indications so far are that it is an attempt to increase the capacity for voluntary assistance to states. We offer no opinion on the value of legislatively making such a designation permanent other than to catalog it here as a concern.

C.4.E. Impact on Preparation for Cyber-Attacks

Critics also point out that the act of designation does not address how the United States would or should react to foreign cyber-attacks.[60] This is true. But designation does help prepare for attacks by re-prioritizing DHS's cybersecurity resources to help EOs should they request it.

C.4.F. Impact on DHS Assistance

Some have correctly observed that since the subsector designation occurred, DHS has offered no assistance other than what it has always offered to the states.[61] However, states have accepted more voluntary aid from DHS and DHS has been more successful at supplying it since the designation -- although it is possible that this was not a result of designation.

C.4.G. Conditions on DHS Assistance

DHS assistance based on voluntary requests from states is a relatively new relationship. Some EOs have expressed concern that such assistance might 1) become contingent on compliance with DHS guidance or conformance to DHS security requirements; or 2) be performed with a scope that is defined by DHS not scoped and constrained by the state requesting assistance.[62] If

---

58 Deborah Barfield Berry "House Panel Votes to Close Election Assistance Commission," *USA Today.* February 7, 2017. https://www.usatoday.com/story/news/politics/2017/02/07/house-panel-votes-close-election-assistance-commission/97603326/

59 "H.R.1562 - SAFE Act." congress.gov, accessed August 16, 2017. http://www.congress.gov/bill/115thcongress/house-bill/1562/all-actions HR 1562 is a bill that seeks to make the designation of election as CI permanent by act of Congress, among other things.

60 Pam Fessler. "State And Local Officials Wary Of Federal Government's Election Security Efforts." National Public Radio, April 5, 2017, http://www.npr.org/2017/04/05/522732036/state-and-local-officials-waryof-federal-governments-election-security-efforts

61 Lily Newman, "Securing Elections Remains Surprisingly Controversial," *Wired*, July 13, 2017, http://www.wired.com/story/election-security-critical-infrastructure/

62 Hans A. von Spakovsky. "Why Does DHS Want to Designate Election Booths 'Critical Infrastructure?' The Heritage Foundation, Aug. 17, 2016, http://www.heritage.org/election-integrity/commentary/why-doesdhs-want-designate-election-booths-critical-infrastructure

such adverse situations were to arise, they would definitely be cases of both overreach of DHS's assistive function and departure from the existing experiences of DHS engagement with other CI sectors. However, the concern is legitimate, not because of past experience, but because elections are a unique government function, and DHS is part of the government that is served by elections. As a result, DHS's relationship with election CI operators might have less clarity than relationships with CI operators in other sectors. Perhaps the best way to address such concerns and maintain vigilance over DHS's role is for states to voluntarily participate in information sharing organizations, sharing experiences pro and con from engagement with DHS.

C.4.H. Constitutionality of Designation

Another criticism of designation is, as some EOs have argued, that the federal government has no constitutional legal authority to classify elections infrastructure as critical infrastructure.[63] It is possible that this is the case, but regardless, it is a constitutional law issue to be dealt with separately from the continuing upsurge in engagement among local, state, and federal government on improving protections to EI.

C.4.I. State Opposition

Another concern, as pointed out by Hans A. von Spakovsky is that "the formal designation itself admitted that 'many [state and local election officials] are opposed to this designation.'"[64] Yet, many find it concerning that a designation claiming to give more resources to states, would be opposed by those same states. This fear likely ties into concern of federal overreach, which has been at least partially allayed by the voluntary nature of DHS assistance. It is also important that as the CI sector develops, new processes, platforms, and policies are put in place to prevent DHS from using its resources as leverage to manipulate elections—that is, appropriate checks and balances.

C.4.J. Necessity of Designation

A final concern, also expressed by von Spakovsky, is that "nothing prevents DHS from making recommendations now —no 'critical infrastructure' designation is required."[65] It is true that assistance can be provided to states without the critical infrastructure designation, but the designation increases the capacity for voluntary information sharing organizations, and prioritizes DHS cybersecurity resources for EI.

Another significant concern about designation is the observation that EI appears to be very different from other existing officially designated CI, in sectors such as transportation, finance, telecom, and others. This is also a reasonable assertion; however, as noted above, there are important similarities to existing CI sectors as well, which can provide a valuable model for uplift of EI protection, and specific measures that are relevant with or without an official designation.

---

63 Mark Rockwell, "Critical infrastructure designation for voting goes too far, says state official," *FCW*, September 13, 2016, http://fcw.com/articles/2016/09/13/election-hack-hearing-rockwell.aspx

64 Hans A. von Spakovsky. "DHS' Election Power-Grab Raises Huge Questions and Red Flags." The Heritage Foundation, Jan. 13, 2017. http://www.heritage.org/election-integrity/commentary/dhs-electionpower-grab-raises-huge-questions-and-red-flags

65 Hans A. von Spakovsky. "Why Does DHS Want to Designate Election Booths 'Critical Infrastructure?' The Heritage Foundation, Aug. 17, 2016, http://www.heritage.org/election-integrity/commentary/why-doesdhs-want-designate-election-booths-critical-infrastructure

Citations

1. "Albert Network Monitoring." *Center for Internet Security*. Accessed on January 16, 2020. https://www.cisecurity.org/services/albert-network-monitoring. In this page the *Center for Internet Security*, the creator of Albert sensors, explains the sensors' purpose and how they function.
2. Bergmann, Max and Carolyn Kenney. "War by Other Means." *Center for American Progress*, June 6, 2017, https://www.americanprogress.org/issues/security/reports/2017/06/06/433345/war-by-other-means/. Bergmann and Kenney's report discusses how liberal democracies are under attack by non-traditional methods, in particular by disinformation. The report focuses specifically on Russia's playbook and the goals of Moscow's operations.
3. Berry, Deborah Barfield. "House Panel Votes to Close Election Assistance Commission." *USA Today*. February 7, 2017. https://www.usatoday.com/story/news/politics/2017/02/07/house-panel-votes-close-election-assistance-commission/97603326/.
4. Bertrand, Natasha. "Russia organized 2 sides of a Texas protest and encouraged 'both sides to battle in the streets.'" *Business Insider*. November 1, 2017. https://www.businessinsider.com/russia-trolls-senate-intelligence-committee-hearing-2017-11.
5. Bump, Philip. "Timeline: How Russian agents allegedly hacked the DNC and Clinton's campaign." *the Washington Post*. July 13, 2018. https://www.washingtonpost.com/news/politics/wp/2018/07/13/timeline-how-russian-agents-allegedly-hacked-the-dnc-and-clintons-campaign/.
6. Cleary, Gillian. "Twitterbots: Anatomy of a Propaganda Campaign." *Symantec*. June 5, 2019. https://www.symantec.com/blogs/threat-intelligence/twitterbots-propaganda-disinformation. Cleary's report reveals new findings about Russia's disinformation campaign during the 2016 US election. Among these findings are that the campaign was both more carefully planned and greater in scale than previously believed.
7. Coats, Daniel R. "Worldwide Threat Assessment." Office of the Director of National Intelligence, January 29, 2019. https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf. The Worldwide Threat Assessment is a long-form, unclassified explanation of the risks facing the United States from the perspective of the US intelligence community. It is requested by the U.S. Senate Select Intelligence Committee and is published by the Director of National Intelligence, in this case former Director Daniel Coats.
8. "Computer Security Resource Center National Vulnerability Database." *National Institute of Standards and Technology*. https://nvd.nist.gov/vuln/search/results?adv_search=true&form_type=advanced&cpe_version=cpe:/o:microsoft:windows_2003_server. The National Vulnerability Database provides a list of common vulnerabilities or exposures (CVEs) for operating systems. This

specific search shows CVEs for Windows operating systems including those implemented with current voting systems.

9. Corse, Alexa and Dustin Volz. "No, You Can't Vote Via Text or Tweet." *The Wall Street Journal*. August 11, 2018. https://www.wsj.com/articles/no-you-cant-vote-via-text-or-tweet-1533985201. This article overviews attempts to persuade voters that they could vote by text, or other forms of illegitimate so-called "voting" in what is believed to be an attempt to suppress votes from specific demographics.
10. "Cybersecurity Assessment." *The Cybersecurity and Infrastructure Security Agency*. Accessed on January 16, 2020. https://www.dhs.gov/cisa/cybersecurity-assessments. This page offers a breakdown of cybersecurity risk assessments offered by CISA.
11. "Develop & Deliver More Secure Solutions." *Intel*. Accessed on January 16, 2020. https://software.intel.com/en-us/sgx. This webpage discusses how Intel is working on developing what it has named the Software Guard Extensions (SGX). SGX has a number of applications outside of election security, but most relevant to this Briefing, it could provide a way for election systems to, at their foundations, improve security.
12. "Election Infrastructure ISAC." *Center for Internet Security*. Accessed on January 16, 2020. https://www.cisecurity.org/ei-isac/. This is the home website of the EI-ISAC. It includes a mission statement as well as members list, which notably includes a number of election system vendors.
13. "Election Technology & the Global Supply Chain," *Interos*, https://cdn2.hubspot.net/hubfs/5812029/Interos%20-%20Election%20Security%20Paper.pdf Interos, a third-party risk management platform, released a report highlighting the supply-chain vulnerabilities of current voting machines.
14. Eric Fisher. "The Designation of Election Systems as Critical Infrastructure." *Congressional Research Service*, January 28, 2019, https://fas.org/sgp/crs/misc/IF10677.pdf. This report from the *Congressional Research Service* explains the implications of election infrastructure being designated as critical infrastructure.
15. Fessler, Pam. "State And Local Officials Wary Of Federal Government's Election Security Efforts." *National Public Radio*. April 5, 2017. www.npr.org/2017/04/05/522732036/state-and-local-officials-wary-of-federal-governments-election-security-efforts. This NPR story examines election officials' concerns about DHS's choice to designate election infrastructure as critical infrastructure. The source provides evidence that, at the time, election officials were concerned that designation might lead to federal regulation of elections and that it did not provide for a response to cyber attacks.
16. "Glossary: National security systems." *Computer Security Resource Center*. Accessed on January 16, 2020. https://csrc.nist.gov/glossary/term/national-security-system#targetText=Any%20information%20system%20(including%20any%20telecommunications%20system)%20used%20or%20operated,national%20defense%20or%20foreign%20opolicy.This source offers a useful definition of national security systems.
17. "Help America Vote Act." *Election Assistance Commission*. Accessed on January 16, 2020. https://www.eac.gov/about/help-america-vote-act. This page on the EAC's website offers an explanation of what the Help America Vote Act (HAVA) is. HAVA was a foundational

piece of legislation for current election infrastructure, as it set in motion federal standards and elections funding practices for years to come.

18. "H.R.1625 - Consolidated Appropriations Act, 2018." Congress.gov. Accessed May 12, 2019, https://www.congress.gov/bill/115th-congress/house-bill/1625/text. The full text of the 2019 Consolidated Appropriations Act, also known as the Omnibus Bill.

19. "H.R.1562 - SAFE Act." *congress.gov*. Accessed August 16, 2017. https://www.congress.gov/bill/115th-congress/house-bill/1562/all-actions. Congress.gov is a website that provides a place to view congressional bills. It tracks the bills' progress through Congress as well as showing their text and other relevant information. This specific page shows HR 1562 and the relevant text regarding the bill's intention to permanently legislate election infrastructure as critical infrastructure. The site illustrates why some might fear that DHS's designation might lead to a permanent designation from Congress.

20. Johnson, Derek. "Officials push for more election security dollars." *FCW*. July 24, 2018. https://fcw.com/articles/2018/07/24/election-security-funding-ogr.aspx. Johnson quotes Chris Krebs as saying that election systems need to be updated across the board, and agreeing that on-going funding will be necessary.

21. Kim, Gene H. and Eugene H. Spafford. "Experiences With Tripwire: Using Integrity Checkers for Intrusion Detection." *Computer Science Technical Report*, Department of Computer Science, Purdue University. 1994. http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=2114&context=cstech. A report from Perdue University that discusses findings regarding the integrity checking program *Tripwire*. It offers an example of how security protocols and techniques that rely on a fundamentally insecure system are limited by the accuracy of inputs.

22. Lindeman, Mark and Philip B. Stark. "A Gentle Introduction to Risk-limiting Audits." *IEEE Security and Privacy*. March 16, 2012. www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf Lindeman and Stark's work offers an explanation of how risk-limiting audits work and why they are important. The article offers a way for interested readers to learn more about RLAs.

23. Lovelace, Alexander. "2016 wasn't the first time Russia tried to sway a US election." *Washington Examiner*. December 29, 2016. https://www.washingtonexaminer.com/2016-wasnt-the-first-time-russia-tried-to-sway-a-us-election. This article from the *Washington Examiner* provides an overview of the history of Russian and Soviet interference in US elections.

24. Manfra, Jeanette. "Jeanette Manfra's Statement for the Record Senate Committee on Homeland Security and Government Affairs." *Senate Committee on Homeland Security and Government Affairs*. April 24, 2018. https://www.hsgac.senate.gov/imo/media/doc/Testimony-Manfra-2018-04-24.pdf. Jeanette Manfra was, at the time of this hearing, the assistant director of CISA, a department within DHS that focuses on cybersecurity and infrastructure security.

25. Meko, Tim, Denise Lu, Lazaro Gamio. "How Trump won the presidency with razor-thin margins in swing states." *The Washington Post*, November 11, 2016. https://www.washingtonpost.com/graphics/politics/2016-election/swing-state-margins

This article from the *Washington Post* explains how Trump was able to win the electoral college on narrow margins in swing states and how a few votes in specific places decided the race.

26. "National Continuity Policy Implementation Plan." Homeland Security Council. August, 2007. https://emilms.fema.gov/IS0545/documents/NCPIP_August_2007_508_Compliant.pdf. On May 4, 2007, President George W. Bush issued "the National Continuity Policy" -- an updated, integrated approach to maintaining a comprehensive and effective continuity capability to ensure the preservation of our constitutional form of government and the continuing performance of National Essential Functions [NEFs] under all conditions. NEFs include "the eight functions the President and national leadership will focus on to lead and sustain the Nation during a catastrophic emergency."

27. Newman, Lily. "Securing Elections Remains Surprisingly Controversial." Wired, July 13, 2017. https://www.wired.com/story/election-security-critical-infrastructure/.

28. Nielsen, Kirstjen. "Written testimony of DHS Secretary Kirstjen Nielsen for a Senate Committee on Homeland Security and Governmental Affairs hearing titled 'Threats to the Homeland.'" *Department of Homeland Security*. October 10, 2018. https://www.dhs.gov/news/2018/10/10/written-testimony-dhs-secretary-kirstjen-nielsen-senate-committee-homeland-security. Nielsen's testimony to Congress reveals DHS's desire to prioritize election security.

29. Perez, Edward and Gregory Miller. "Reinventing the U.S. Election Assistance Commission." *OSET Institute*. December 2019. https://www.osetfoundation.org/research/2019/08/08/reinventingeac. Perez and Miller's piece covers a number of flaws and potential solutions in the current U.S. EAC, expanding upon the findings and recommendations found in this briefing.

30. "Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure." *Office of the Inspector General Department of Homeland Security*. February 28, 2019. https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-24-Feb19.pdf. This DHS report assesses the state of risk to election infrastructure. Among other things it mentions the deployment of 100 Albert sensors across 40 states.

31. "Presidential Decision Directive 63." Clinton Digital Library. May 20, 1998. https://clinton.presidentiallibraries.us/items/show/12762. This Presidential Directive during the Clinton administration established critical infrastructure. At the time the designation did not extend to election infrastructure.

32. "Presidential Policy Directive—Critical Infrastructure Security and Resilience (Presidential Policy Directive/PPD-21)." February 12, 2013. February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

33. Rebello, Keith. "System Security Integration Through Hardware and Firmware." *DARPA*. https://www.darpa.mil/program/system-security-integration-through-hardware-and-firmware DARPA's System Security Integration Through Hardware and Firmware (SSITH) program aims to create a hardware security architecture to reduce potential software

exploitation. The goal is to protect systems from privilege, permission, memory error, information leakage, and code injection exploitations.

34. Richell, Tom. "Midterm elections: Voting machine automatically selects Republican candidate instead of Democrat in Indiana, video shows." *The Independent*. November 7, 2018. https://www.independent.co.uk/news/world/americas/us-politics/midterms-2018/midterms-elections-video-voting-machine-malfunction-indiana-democrat-republican-a8621101.html. Reports during the 2018 midterm elections alleged that voting machines were selecting Republican candidates over Democratic candidates in Indiana.

35. Rockwell, Mark . "Critical infrastructure designation for voting goes too far, says state official." *FCW*. September 13, 2016. https://fcw.com/articles/2016/09/13/election-hack-hearing-rockwell.aspx. Rockwell's article gives voice to the officials who were initially concerned that the designation of election infrastructure as critical infrastructure was unnecessary and could lead to federal overreach. The article provided evidence that some officials believed that the critical infrastructure designation was unconstitutional.

36. Satter, Raphael. "Inside story: How Russians hacked the Democrats' emails." *Associated Press*. November 4, 2017. https://www.apnews.com/dea73efc01594839957c3c9a6c962b8a. Satter's article retells how Russian agents infiltrated John Podesta's emails during the 2016 U.S. presidential election campaign.

37. Schlesinger, Robert. "Hack the Vote: a reminder of how insecure our ballots can be." *U.S. News & World Report*. July 31, 2017. https://www.usnews.com/opinion/thomas-jefferson-street/articles/2017-07-31/hackers-demonstrate-how-vulnerable-voting-machines-are. Many demonstrations by hackers, both in interviews and at conferences, have demonstrated the ease with which a skilled adversary can compromise the integrity of a voting machine. Schlesinger's article documents one such conference.

38. Sebes, John and Cliff Wulfman. "Online Voter Registration Systems: Best Practices." *OSET Institute*. March 5, 2018. https://ww.osetfoundation.org/research/2017/9/11/critical-democracy-infrastructure-yss33. This OSET Institute briefing discusses both how online voter registration (OVR) can improve U.S. election administration, as well as how best to implement OVR.

39. "Securing Elections as Critical Infrastructure." *National Association of Secretaries of State*. Accessed August 17, 2017. https://www.nass.org/index.php/nass-initiatives/nass-cybersecurity-elections-critical-infrastructure/. This webpage offers the NASS's views on the designation of election infrastructure as critical infrastructure and makes very clear that, at the time of the designation, many states were against it. The page was useful for providing evidence that critics of the critical infrastructure designation believed that the designation was unclear about its scope.

40. "Securing the Vote." *The National Academies of Science Engineering and Medicine*. 2018. Y https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy Securing the Vote, a report from the *National Academies*, evaluates the state of U.S. election infrastructure in the wake of the 2016 election and offers a series of recommendations for a variety of stakeholders (the federal government, local governments, election system vendors, etc.) for how to improve election security.

41. Spakovsky, Hans. “DHS' Election Power-Grab Raises Huge Questions and Red Flags.” *The Heritage Foundation*. January 13, 2017. https://www.heritage.org/election-integrity/commentary/dhs-election-power-grab-raises-huge-questions-and-red-flags. Spakovsky’s article offers a critical take on the designation of election as critical infrastructure. It relies heavily on EAC commissioner Christy McCormick’s initial views of the designation. The article raised concerns over whether the designation was necessary and the fact that many state officials disapproved of it.

42. Spakovsky, Hans. “Why Does DHS Want to Designate Election Booths 'Critical Infrastructure?' *The Heritage Foundation*. August 17, 2016. https://www.heritage.org/election-integrity/commentary/why-does-dhs-want-designate-election-booths-critical-infrastructure. Spakovsky’s other article is also critical of the critical infrastructure designation. He raised concerns that the designation would allow public officials to play a malicious role in elections. The article provides a voice to concerns that the designation was unnecessary and that DHS’s assistance, while technically voluntary, might in effect be compulsory.

43. Starks, Tim. “DHS labels elections as 'critical infrastructure.” *Politico*, January 6, 2017. https://www.politico.com/story/2017/01/elections-critical-infrastructure-homeland-security-233304. Starks’s article describes the designation of election infrastructure as critical infrastructure and the criticisms that came with the designation. The article references Georgia’s then-Secretary of State Brian Kemp’s disagreement with the designation.

44. “Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector.” *Department of Homeland Security*. January 6, 2017. https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designationelection-infrastructure-critical. Here Jeh Johnson, then-Secretary of Homeland Security, officially announces the designation of election infrastructure as critical infrastructure.

45. “The Constitution of the United States: A Transcription.” *National Archives*. June 26, 2017. https://www.archives.gov/founding-docs/constitution-transcript. This website offers a full transcript of the United States Constitution. Certain articles and amendments to the Constitution describe the laws regarding federal elections.

46. Timberg, Craig. “Russian propaganda effort helped spread ‘fake news’ during election, experts say.” *The Washington Post*. November 24, 2016. https://www.washingtonpost.com/business/economy/russian-propaganda-effort-helped-spread-fake-news-during-election-experts-say/2016/11/24/793903b6-8a40-4ca9-b712-716af66098fe_story.htm.

47. “What Is Critical Infrastructure?” *Department of Homeland Security*. July 12, 2017. https://www.dhs.gov/whatcritical-infrastructure. This page from DHS offers the definition of critical infrastructure used by the Department.

48. “2018 Election Administration & Voting Survey.” *Election Assistance Commission*. Accessed January 16, 2020. https://www.eac.gov/research-and-data/election-administration-voting-survey This page on the EAC website explains the basic purpose and goal of the Election Administration & Voting Survey and offers additional information about the survey.

Glossary of Terms

The definitions in this Glossary for terms appearing in this Briefing were derived from language enacted in federal laws and/or included in National Plans, including:

- Homeland Security Act of 2002
- USA PATRIOT Act of 2001
- 2013 NIPP (*heavily relied upon for this Briefing*)
- Presidential Policy Directive #8 (PPD-8), National Preparedness
- Presidential Policy Directive #21 (PPD-21), Critical Infrastructure Security and Resilience

Additional definitions come from the DHS Lexicon. The source for each entry below follows each definition. Terms appearing in the Briefing that appear below have the meaning as defined hereunder unless otherwise attributed or explained by footnote.

Asset. A person, structure, facility, information, material, or process that has value. (*Source: DHS Lexicon, 2010*)

Business Continuity. Activities performed by an organization to ensure that during and after a disaster the organization's essential functions are maintained uninterrupted, or are resumed with minimal disruption. (*Source: 2013 NIPP*)

Consequence. The effect of an event, incident, or occurrence, including the number of deaths, injuries, and other human health impacts along with economic impacts both direct and indirect and other negative outcomes to society. (*Source: DHS Lexicon, 2010*)

Control Systems. Computer-based systems used within many infrastructure and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (*operators*). Examples of types of control systems include SCADA systems, Process Control Systems, and Distributed Control Systems. (*Source: 2013 NIPP*)

Critical Infrastructure. Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (*Source: §1016(e) of the USA Patriot Act of 2001 (42 U.S.C. §5195c(e))*

Critical Infrastructure Community. Critical infrastructure owners and operators, both public and private; Federal departments and agencies; regional entities; SLTT governments; and other organizations from the private and nonprofit sectors with a role in securing and strengthening the resilience of the Nation's critical infrastructure and/or promoting practices and ideas for doing so. (*Source: 2013 NIPP*)

Critical Infrastructure Information (CII). Information that is not customarily in the public domain and is related to the security of critical infrastructure or protected systems. CII consists of records and information concerning any of the following:

- Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law; harms the interstate commerce of the United States; or threatens public health or safety.
- The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation, risk management planning, or risk audit.
- Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, insurance, or continuity, to the extent that it is related to such interference, compromise, or incapacitation. (*Source: CII Act of 2002, 6 U.S.C. § 131*)

Critical Infrastructure Owners and Operators. Those entities responsible for day-to-day operation and investment of a particular critical infrastructure entity. (*Source: 2013 NIPP*)

Critical Infrastructure Partner. Those Federal and SLTT governmental entities, public and private sector owners and opera- tors and representative organizations, regional organizations and coalitions, academic and professional entities, and certain not-for-pro t and private volunteer organizations that share responsibility for securing and strengthening the resilience of the Nation's critical infrastructure. (*Source: 2013 NIPP*)

Critical Infrastructure Partnership Advisory Council (CIPAC). Council established by DHS under 6 U.S.C. §451 to facilitate effective interaction and coordination of critical infrastructure activities among the Federal Government; the private sector; and SLTT governments. (*Source: CIPAC Charter*)

Critical Infrastructure Risk Management Framework. A planning and decision-making framework that outlines the process for setting goals and objectives, identifying infrastructure, assessing risks, implementing risk management activities, and measuring effectiveness to inform continuous improvement in critical infrastructure security and resilience. (*Source: 2013 NIPP*)

Cybersecurity. The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wire-line, wireless, satellite, public safety answering points, and 911 communications systems and control systems. (*Source: 2013 NIPP*)

Cyber System. Any combination of facilities, equipment, personnel, procedures, and communications integrated to pro- vide cyber services; examples include business systems, control systems, and access control systems. (*Source: 2013 NIPP*)

Dependency. The one-directional reliance of an asset, system, network, or collection thereof—within or across sectors—on an input, interaction, or other requirement from other sources to function properly. (*Source: 2013 NIPP*)

Executive Order 13636. Executive Order that calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cybersecurity information sharing; develop a technology-neutral cybersecurity frame- work; and promote and incentivize the adoption of strong cybersecurity practices. (*Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 2013, Executive Order 13636, www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf*)

Emergency Support Functions (ESF). The primary, but not exclusive, Federal coordinating structures for building, sustaining, and delivering the response core capabilities. ESFs are vital for responding to Stafford Act incidents but also may be used for other incidents. (*Source: National Response Framework, 2013*)

Federal Departments and Agencies. Any authority of the United States that is an "agency" under 44 U.S.C. §3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. §3502(5). (*Source: PPD-21, 2013*)

Incident. An occurrence, caused by either human action or natural phenomenon, that may cause harm and require action, which can include major disasters, emergencies, terrorist attacks, terrorist threats, attacks, cyber failure or accident, and other occurrences requiring an emergency response. (*Source: DHS Lexicon, 2010*)

Information Sharing and Analysis Centers (ISACs). Operational entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24x7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders. (*Source: PDD-63, 1998*)

Information Sharing and Analysis Organization. Any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of:

(a) Gathering and analyzing critical infrastructure information to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof;

(b) Communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or an incapacitation problem related to critical infrastructure or protected systems; and

(c) Voluntarily disseminating critical infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (a) and (b). (*Source: Homeland Security Act of 2002, 6 U.S.C. § 131*)

Infrastructure. The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and

society as a whole; consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements. (*Source: DHS Lexicon, 2010*)

Interdependency. Mutually reliant relationship between entities (objects, individuals, or groups); the degree of interdependency does not need to be equal in both directions. (*Source: DHS Lexicon, 2010*)

Joint Terrorism Task Forces (JTTFs). FBI-led local task forces of highly trained Federal, State, and local law enforcement and intelligence agencies established to collect terrorism-related intelligence and conduct investigations. The local FBI JTTFs receive and resolve reports of possible terrorism activity submitted by private industry partners and the public. (*Source: FBI Website, www.fbi.gov*)

Mitigation. Capabilities necessary to reduce loss of life and property by lessening the impact of disasters. (*Source: PPD-8, 2011*)

National Cyber Investigative Joint Task Force. The multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from Federal agencies, including DHS, and from State, local, and international law enforcement partners. (*Source: FBI Website, www.fbi.gov*)

National Cybersecurity and Communications Integration Center. The national cyber critical infrastructure center, as designated by the Secretary of Homeland Security, which secures Federal civilian agencies in cyberspace; provides support and expertise to private sector partners and SLTT entities; coordinates with international partners; and coordinates the Federal Government mitigation and recovery efforts for significant cyber and communications incidents. (*Source: DHS Website, www.dhs.gov*)

National Infrastructure Coordinating Center. The national physical critical infrastructure center, as designated by the Secretary of Homeland Security, which coordinates a national network dedicated to the security and resilience of critical infrastructure of the United States by providing 24/7 situational awareness through information sharing, and fostering a unity of effort. (*Source: DHS Website, www.dhs.gov*)

National Operations Center. A DHS 24x7 operations center responsible for providing real-time situational awareness and monitoring of the homeland, coordinating incident response activities, and, in conjunction with the Office of Intelligence and Analysis, issuing advisories and bulletins concerning threats to homeland security, as well as specific protective measures. (*Source: DHS Website, www.dhs.gov*)

National Preparedness. The actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. (*Source: PPD-8, 2011*)

Network. A group of components that share information or interact with each other to perform a function. (*Source: 2013 NIPP*)

Partnership. Close cooperation between parties having common interests in achieving a shared vision. (*Source: 2013 NIPP*)

Presidential Policy Directive 8 (PPD-8). Facilitates an integrated, all-of-Nation approach to national preparedness for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, attacks, pandemics, and catastrophic natural disasters; directs the Federal Government to develop a national preparedness system to build and improve the capabilities necessary to maintain national preparedness across the five mission areas covered in the PPD: prevention, protection, mitigation, response, and recovery. (*Source: PPD-8, 2011*)

Presidential Policy Directive 21 (PPD-21). Aims to clarify roles and responsibilities across the Federal Government and establish a more effective partnership with owners and operators and SLTT entities to enhance the security and resilience of critical infrastructure. (*Source: The White House, Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience, www.whitehouse.gov/the-press-office/2013/02/12/ presidential-policy-directive-critical-infrastructure-security-and-resil, 2013*)

Prevention. Those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. (*Source: PPD-8, 2011*)

Protected Critical Infrastructure Information (PCII). All critical infrastructure information that has been properly submitted and validated pursuant to the Critical Infrastructure Information Act and implementing directive; all information submit- ted to the PCII Program Office or designee with an express statement is presumed to be PCII until the PCII Program Office determines otherwise. (*Source: CII Act of 2002, 6 U.S.C. § 131*)

Protection. Those capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters. (*Source: PPD-8, 2011*)

Recovery. Those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources. (*Source: PPD-8, 2011*)

Recovery Support Functions (RSF). Coordinating structures for key functional areas of assistance during recovery operations; RSFs support local governments by facilitating problem solving, improving access to resources, and fostering coordination among State and Federal agencies, nongovernmental partners, and stakeholders. (*Source: National Disaster Recovery Framework, 2011*)

Resilience. The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. (*Source: PPD-21, 2013*)

Response. Capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred. (*Source: PPD-8, 2011*)

Risk. The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. (*Source: DHS Lexicon, 2010*)

Risk-Informed Decision Making. The determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, and other relevant factors. (*Source: 2013 NIPP*)

Sector. A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society; the *National Plan* addresses 16 critical infrastructure sectors, as identified in PPD-21. (*Source: 2013 NIPP*)

Sector Coordinating Council (SCC). The private sector counterpart to the GCC, these councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector; serve as principal entry points for the government to collaborate with each sector for developing and coordinating a wide range of critical infrastructure security and resilience activities and issues. (*Source: 2013 NIPP*)

Sector-Specific Agency (SSA). A federal department or agency designated by PPD-21 with responsibility for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. (*Source: PPD-21, 2013*)

Sector-Specific Plans (SSP). Planning documents that complement and tailor application of the *National Plan* to the specific characteristics and risk landscape of each critical infrastructure sector; developed by the SSAs in close collaboration with the SCCs and other sector partners. (*Source: Adapted from the 2013 NIPP*)

Secure/Security. Reducing the risk to critical infrastructure by physical means or defensive cyber measures to intrusions, attacks, or the effects of natural or manmade disasters. (*Source: PPD-21, 2013*)

Steady State. The posture for routine, normal, day-to-day operations as contrasted with temporary periods of heightened alert or real-time response to threats or incidents. (*Source: DHS Lexicon, 2010*)

System. Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose. (*Source: DHS Lexicon, 2010*)

Terrorism. Premeditated threat or act of violence against noncombatant persons, property, and environmental or economic tar- gets to induce fear, intimidate, coerce, or affect a government, the civilian population, or any segment thereof, in furtherance of political, social, ideological, or religious objectives. (*Source: DHS Lexicon, 2010*)

Threat. A natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. (*Source: DHS Lexicon, 2010*)

Threat and Hazard Identification and Risk Assessment (THIRA). A tool that allows a regional, State, or urban area jurisdiction to understand its threats and hazards and how the impacts may vary according to time of occurrence, season, location, and other community factors. This knowledge helps a jurisdiction establish informed and defensible capability targets for prepared- ness. (*Source: www.fema.gov*)

Value Proposition. A statement that outlines the business and national interest in critical infrastructure security and resilience actions and articulates the benefits gained by partners through collaborating in the mechanisms described in the *National Plan*. (*Source: 2013 NIPP*)

Vulnerability. A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. (*Source: DHS Lexicon, 2010*).

Acknowledgements

As with the last edition in 2017, OSET Institute Board member **Peter F. Harter** provided guidance and advice in the development of this work. Several Board Advisors contributed key advice and input on the subject matter, including **Cameron Quinn**, a lifelong election administration executive and lawyer now with the Department of Homeland Security; **Aneesh Chopra**, former U.S. CTO; **Dr. Rich DeMillo**, Distinguished Professor of Computing and Professor of Management at the Georgia Institute of Technology; **Dr. David Bader**, Distinguished Professor and Director of the Institute for Data Science at the New Jersey Institute of Technology; and **Simon Rosenberg**, President of the New Policy Institute.

We gratefully acknowledge and thank **Dr. R. David Edelman**, former Special Assistant to President Obama for Economic & Technology Policy (*and previously served on President Obama's National Security Council staff as Director for International Cyber Policy and in the Office of Science & Technology Policy*), and directs the Project on Technology, the Economy, and National Security (TENS) at the Massachusetts Institute of Technology. Dr. Edelman was the principal catalyst for the development of the original version of the Critical Democracy Infrastructure Briefing during his White House tenure in August of 2016.

We also are grateful to a list of over 100 elections experts and officials who, over the course of the past 3 years from time to time, provided insights, knowledge, and opinions through informal conversations, interviews, articles, postings, and replies in digital media, and/or other exchanges of mindshare that helped shape this 2nd edition of the CDI Briefing. We wanted to include anyone we spoke with or participated in digital communications with about this work, including: **Kim Alexander**, Executive Director, California Voter Foundation; **William Anthony**, Director, Franklin County Ohio Board of Elections; **Andrew Appel**, Professor of Computer Science, Princeton University; **Ron Bandes**, Network Security Analyst, Software Engineering Institute, CERT Division; **Josh Benaloh**, Research Scientist, Microsoft Research; **Kenneth Bennett**, Office of Registrar-Recorder/County Clerk, Los Angeles County, CA; **Matt Bishop**, Professor of Computer Science, University of California Davis; **Kimball Brace**, Election Data Services, Inc.; **Harvey Branscomb**, Coloradans for Voting Integrity; **Doug Chapin**, Director of the Program for Excellence in Election Administration, Humphrey School of Public Affairs, University of Minnesota; **Matthew Caufield**, Ph.D Cnd., Wharton School; **Dana Chisnell**, Co-Director, Center for Civic Design; **Thomas E. Connolly**, Deputy Director of Public Information, New York State Board of Elections; **Dr. Andrew Coopersmith**, Managing Director, Penn-Wharton Public Policy Institute; **Dana DeBeauvoir**, Clerk, Travis County Texas; **David Dill**, Professor of Computer Science, Stanford University; **Caitlin Dirkovich**, Toffler Associates; **Hon. Matthew Dunlap**, Maine Secretary of State; **Susan Dzieduszycka-Suinat**, President and CEO, Overseas Vote Foundation; **John Dziurlaj**, former IT Data Architect, Office of Secretary of State, Ohio; **Mark Earley**, Voting Systems Manager, Leon County Florida Board of Elections; **Jeremy Epstein**, Deputy Division Director, Computer & Network Systems Division, National Science Foundation; **Edward Felten**, Professor of Computer Science, Princeton University; **Christopher Fowler**, Chief Innovation Officer and Director of IT, Rhode Island Department of State; **Josh Franklin**, U.S. Election Assistance Commission; **Susannah Goodman**, Director for Corporate Accountability, Common Cause; **Hon. Nellie Gorbea**, Rhode Island Secretary of State; **Susan Greenhalgh**, Elections Specialist, NEDC; **Alex Halderman**, Director, Center for Computer Security and Society, University of Michigan; **Thomas Hicks**, Commissioner, U.S. Election Assistance Commission; **Candice Hoke**, Professor, Cleveland State University and Center for Election Excellence; **Gema Howell**, National Institute of Standards and Technology; **Harri Hursti**, Independent Consultant; **Waldo Jaquith**, U.S. Open Data Institute; **David Jefferson**, Visiting Scientist Retired, Lawrence Livermore National Laboratory; **Neil Jenkins**, Chief of Policy and Planning, Department of Homeland Security, National Protection and Programs Directorate, Office of Cybersecurity & Communications.; **Chris Jerdonek**, former President San Francisco Elections Commission; **Douglas Jones**, Professor of Computer Science, University of Iowa; **Arthur Keller**, former Senior Research Scientist, Stanford University; **Neal Kelley**, Registrar, Orange County California; **Doug Kellner**, Co-Chair, New York State Board of Elections; **Joe Kiniry**, Chief Scientist, Galois Inc. and Free and Fair Inc.; **Sharon Laskowski**, National Institute of Standards and Technology; **Dean Logan**, Registrar-Recorder/County Clerk, Los Angeles County California; **Joseph Lorenzo Hall**, Chief Technologist, Center for Democracy and Technology; **Matthew Masterson**, Department of Homeland Security; **Neal McBurnett**, Consultant, Data Science; **John McCarthy**, Computer Scientist, Verified Voting; **Christy McCormick**, Commissioner, U.S. Election Assistance Commission; **Amber McReynolds**, President, National Vote at Home Institute; **Justin Moore**, Computer Scientist, Google, Inc.; **Peter G. Neumann**, Senior Principal Scientist, SRI International; **Lawrence Norden**, Deputy Director, Democracy Program at Brennan

Center for Justice, NYU School of Law; **Whitney Quesenbery**, Co-Director, Center for Civic Design; **Andrew Regenscheid**, National Institute of Standards and Technology; **Ronald L. Rivest**, Vannevar Bush Professor of Electrical Engineering and Computer Science, Massachusetts Institute of Technology; **Joe Rozell**, Director of Elections, Oakland County Michigan Elections Commission; **Ion Sancho**, Supervisor of Elections, Leon County, Florida; **Barbara Simons**, Voting Technology Expert, and Past President, Association for Computing Machinery; **Pamela Smith**, former President, Verified Voting; **Philip Stark**, Professor of Statistics, University of California Davis; **Anthony Stevens**, New Hampshire Office of Secretary of State; **Warren Stewart**, Communications Director, Verified Voting; **Vanessa Teague**, Senior Lecturer, Computing Information Systems, University of Melbourne; **Hon. Maggie Toulouse Oliver**, New Mexico Secretary of State; **Poorvi Vora**, Professor, Computer Science, George Washington University; **Dan Wallach**, Professor of Computer Science, Rice University.

OSET Institute Supporter Acknowledgement

The OSET Institute deeply appreciates the **John S. and James L. Knight Foundation**, the **Democracy Fund**, the **Frost Foundation**, the **James H. Clarke Foundation**, the **Chris Kelly & Jennifer Carrico Families**, the **Barbara Coll Family**, the **Michael L. Henry Family**, **Matt Mullenweg**, the **Frank J. Santoro Family**, and the **Alec Totic Family** for their generous support of our work to increase integrity, lower cost, and improve usability of election technology infrastructure in the U.S. and abroad.

About the Authors

Gregory A. Miller co-founded the Open Source Election Technology (OSET) Institute in November 2006. He leads all aspects of the Institute's resource development, corporate partner R&D alliances, public outreach, election official stakeholder relations, and government and legal affairs. Gregory has been a volunteer subject matter expert in elections technology integrity and security to the U.S. Department of Homeland Security (DHS), the National Security Council (NSC) and continues to advise committees and members of Congress on the same. Mr. Miller has 35+ years of technical and business experience in computer and information technology with Internet and technology pioneers such as Apple, Computervision, Netscape Communications, Sun Microsystems, and Tektronix. He is a trained computer scientist and software engineer, with graduate business education, and his law degree focused on intellectual property, technology law, and public policy. Greg has also been active in the American Bar Association focused on technology law and public policy issues, including Cyber-law, Information Privacy & Security, and Internet Governance. Mr. Miller participated in initial reviews of technology public policy components of the first National Infrastructure Protection Plan in the early 2000. Greg is also a member of the Congressional Internet Caucus Advisory Committee, and a sustaining member of the Internet Society. Mr. Miller also served on the San Francisco Voting Systems Task Force, holding one of the two computer science seats on the Commission, 2010-2012.

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.

E. John Sebes is one of the two original co-founders and Chief Technology Officer ("CTO") for the U.S. based OSET Institute, a nonprofit, nonpartisan election technology research and development organization. He leads all aspects of technology strategy, vision, architecture, engineering and development for the TrustTheVote Project, which is developing ElectOS™ a publicly available, open source election operating system. For over three decades, John has been a software engineer, technical consultant, and CTO, working in several areas—network infrastructure, application frameworks, embedded systems, critical infrastructure, and data center operations — with strong common themes of risk management, security, privacy, and reliability. Innovation and technology transfer have been another consistent theme, in settings as varied as government-funded R&D, venture-backed start-ups, professional services, academia, and non-profits. John has been a Principal Investigator in R&D projects, ranging from DARPA projects performed in the pre-web era, to recent work with the Department of Homeland Security on open source technology. (*Continues*...)

Authors, continued…

E. John Sebes, **continued**: John's involvement with cyber critical infrastructure protection dates back to 2000, when Mr. Sebes was a member of the group who reviewed the first-ever *National Infrastructure Protection Plan* (NIPP), and contributed to the first revision of it, focusing on the infrastructure sectors containing cyber-physical system risks. John is a co-author of 12 patents and 20+ publications.

Sergio Valente is an Election Infrastructure Policy Analyst jointly appointed in the Office of CTO and the Government Relations team of the Office of General Counsel for the OSET Institute. He will earn his undergraduate degree at American University in International Relations and Economics this Spring 2020, and will start law school at Stanford in the fall. Sergio began as an intern at the Institute in 2016, and since then has handled numerous research assignments and participated in development of policy papers for the Institute including, research contributions to first version of this Critical Democracy Infrastructure Briefing; authoring *Protecting Elections As a Matter of National Security*; and publishing several blog posts including a series on the challenges of Internet Voting. Sergio was a significant contributor and initial draftsman of this 2nd version of the CDI Briefing. Beyond his work at the OSET Institute and aside from his academic studies, Sergio interned at the German Marshall Fund, and is, at this writing, interning in the U.S. State Department's Bureau of Intelligence and Research, in the Office of Analytic Outreach. Sergio also spent a semester in Amman, Jordan studying Arabic, and a year in Rome, Italy studying Italian.

OSET Institute Team Acknowledgement

The authors gratefully acknowledge the assistance during the year this Briefing has been in development from **Dennis Mema**, *Policy Analyst* on the Government Relations Team in the Office of General Counsel for the OSET Institute; **Dr. Cliff Wulfman**, *Sr. Member of Technical Staff* in the Office of CTO for the OSET Institute; **Joy London**, *Associate General Counsel & Director International Development* for the OSET Institute, and co-author on the first edition of this CDI Briefing; and the editorial support of Institute and TrustTheVote Project staff, including **Meegan Gregg** and **Susie Derrington**.

14 Years of dedication to innovating public election technology

530 Lytton Avenue
2nd Floor
Palo Alto, California 94301 USA
650.600.1450
www.osetfoundation.org