Georgia Tech | Center for Advanced Communications Policy

US Voting Systems Security Working Paper: "Revisioning the U.S. Elections Process: Voting Security and Election Integrity" Georgia Institute of Technology[1]

June 1, 2019

1.0 Introduction: Revisioning the U.S. Elections Process: Voting Security and Election Integrity

Concerns about the overall integrity of the U.S. electoral system have been raised in light of recent events including the real (and perceived) vulnerabilities of voting technologies (in all forms), as well as the possible interference in U.S. voting by external actors. These questions have been further intensified by the social, political and process complexities of the U.S. electoral system. These perceptions of, and certainty in, the security of electoral processes[2] have significant impact on public confidence in electoral system integrity. The objective of this paper is to clearly articulate the various dimensions of security in a comprehensive manner, while taking into consideration other key system objectives such as accessibility, usability and transparency. Any meaningful conversation on ensuring the security and reliability of the voting process needs to be based on fact and empirical evidence rather than "conventional wisdom." This is true regardless of whether the underlying technologies are digital or paper based.

In terms of electorate messaging, election officials have become sensitive to the fact that *perceived* security can be as critical a variable as *actual* technological security to address in terms of communication with the general public[3]. Public perceptions have been influenced by reporting in the popular press about troubling, though frequently incompletely reported or interpreted findings regarding voting systems, especially the security of voting technologies. Election officials need to be aware of the changing "temperature" of public opinion as it can affect the element of "trust" in the electoral system, a frequently overlooked element of security.

Finally, voting officials are increasingly overwhelmed with a flood of often conflicting, highly technical information on the many aspects of voting security, ranging from machine failure to larger scale election security concerns. This has the very real effect of impeding robust objective discussion and decision-making on election and voting systems acquisition, which can contribute to undermining the credibility of election technology. This whitepaper outlines key dimensions of the security of U.S. voting systems, and focuses on the value of articulating a comprehensive approach that integrates the roles of technology, policy, and communications toward developing and implementing secure, and reliable voting processes

2.0 State of U.S. voting systems and voting technology: Key Issues

The electoral system in the United States is structurally complicated, intensified by electoral, political and technological factors at local, state and national levels. Coupled with an aging and antiquated national electoral infrastructure in many jurisdictions, these factors challenge voter security perceptions, confidence and trust in the integrity of the electoral system.

[1] For more information, or to comment on this paper, contact Paul M.A. Baker, Ph.D., Georgia Tech, [paul.baker@gatech.edu]. We acknowledge the support of the Smartmatic Corporation in conducting this research.

[2] See Darnolf (2018); Rid & Buchanan (2018)

[3] Agawu, E.A. (2018)

Nationally, there is not a standard method of voting, and beyond the rise of early, absentee and mail voting, the means by which Americans vote on Election Day have changed dramatically over the past generation[4] which also increases the complexity of managing security risks. Even though the decentralized system of counting votes compensates by making it harder to tamper with election outcomes[5], this does not ensure complete security, a fact that election officials take very seriously. Security assessments, as currently implemented, are managed somewhat inconsistently nationwide, even among counties with the same election regulations and voting systems. Certification of systems at Federal and State level, provide a certain level of confidence that the systems will work as intended, and while the process addresses basic security issues, this process is not sufficient. On the downside, certification can often have the undesirable effect of inhibiting broad innovation of new systems, and to some extent, of needed or desired changes and updates[6]. Further, this regulatory consideration could also dampen the ability of manufacturers to generate new *security* related innovations.

In this context, only a few jurisdictions (e.g. Los Angeles County) have taken to designing and implementing their own systems, often because they do not view the current market offerings as tailored to their needs in terms of functionality and security[7]. While on the upside, this can result in systems that closely address their needs, it requires a considerable amount of time, money and know-how that not all jurisdictions across the country have.

After a jurisdiction has decided to replace a voting system, they need to consider a variety of factors critical to conducting a successful procurement. Regarding security, they face four main challenges:

1. *Ease of Assessing Security:* This is a variable that basically measures how much money, time, and specialized resources are required to assess whether a system is secure or not. If for example, a jurisdiction requires very little of these resources to assess the security of a solution, then it scores very high in that aspect. If on the other hand, in the case of jurisdictions that build their own systems, security assessment requires a lot of time, investment and hiring specialized expertise, then it scores very low in this aspect.

2. *Effectiveness of Security Assessment:* Regardless of the ease of assessing the security of a voting system, this aspect measures the *effectiveness* of the assessment. It is very easy (low cost, quick, requires no specialized personnel) to just ask a vendor: “Is the system secure?” and then take that answer as a given. The problem here is that this reduces the objective certainty as to whether a voting system fully addresses all aspects of security. Conversely, if a jurisdiction hires a team of consultants for a year, and conducts a full audit on the voting system, this would likely yield a more realistic picture of the systems’ security. This is an expensive option.

3. *Communication:* Full transparency with respect to electoral process security issues, is desirable, however not clearly conveying the complexities of security in difficult conditions (i.e. real or perceived security weakness, technological errors, etc.) potentially opens them to questions of confidence or even competence. And, publicly explaining about the robustness of voting system risks undermining voter confidence and trust in the voting process, and could even depress turnout, if not done properly.

4. *Usability/accessibility*: All voting systems, electronic or otherwise, ideally are designed in a way that usability issues and human error are minimized. Increasing security in a comprehensive manner need not minimize the importance of these accessibility and usability aspects. As noted

[4] Pew (2016b)

[5] Leovy (2017)

[6] University of Pennsylvania (2016)

[7] Norden & Famighetti (2015)

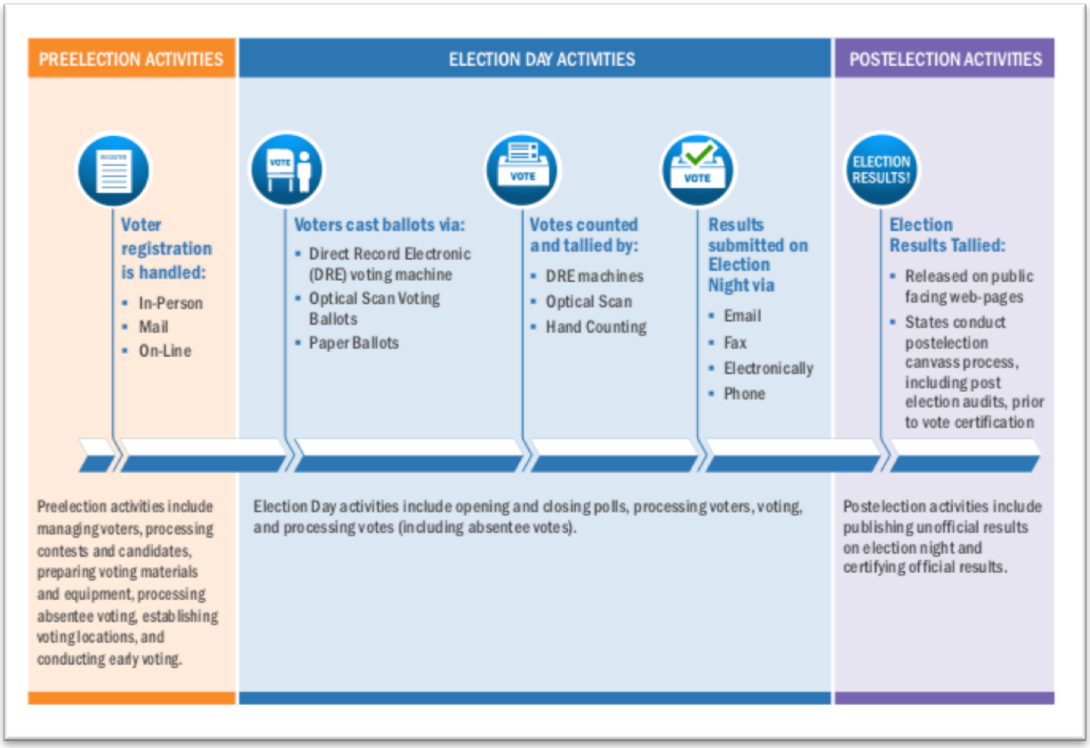
by EAC Chairman Thomas Hicks and Vice Chair Christy McCormick […] "Much of the public discourse around elections since the 2016 Federal election has focused on security – and for good reason. However, increased protections cannot come at the expense of limiting accessibility for voters with disabilities. As we look ahead to the coming year, including the 2018 Federal election, the EAC is committed to ensuring voting systems remain secure while allowing for the highest possible participation for voters with disabilities."[8]

3.0 Critical System Elements: Technological Security, Policy Considerations, Communication Channels

Security, as a key aspect of the voting process, has a number of interrelated aspects and components. Any discussion of security needs to address a number of these dimensions, including:

- Scope (for instance, voter registration, tabulation, auditing of results) of the system.
- Conceptual aspects of security (e.g. physical versus "social hacking", human errors, etc.)
- Level (or phase) of the system under discussion.
- Associated concerns, such as privacy, or technical requirements of security.
- Security policy: issues, barriers, opportunities.
- Role of communication and outreach.

Regarding the *Scope* element, the Department of Homeland Security's infographic[9] (Figure 1) depicts a high-level overview of the key components of the electoral process, which also points to areas in which **assessments and audits** should be considered. This framework could be used as a starting point for developing a comprehensive baseline for any security assessment.


PREELECTION ACTIVITIES
ELECTION DAY ACTIVITIES
POSTELECTION ACTIVITIES
REGISTER
VOTE
VOTE
VOTE
ELECTION RESULTS!
Voter registration is handled:
In-Person
Mail
On-Line
Voters cast ballots via:
Direct Record Electronic (DRE) voting machine
Optical Scan Voting Ballots
Paper Ballots
Votes counted and tallied by:
DRE machines
Optical Scan
Hand Counting
Results submitted on Election Night via
Email
Fax
Electronically
Phone
Election Results Tallied:
Released on public facing web-pages
States conduct postelection canvass process, including post election audits, prior to vote certification
Preelection activities include managing voters, processing contests and candidates, preparing voting materials and equipment, processing absentee voting, establishing voting locations, and conducting early voting.
Election Day activities include opening and closing polls, processing voters, voting, and processing votes (including absentee votes).
Postelection activities include publishing unofficial results on election night and certifying official results.

[8] https://www.eac.gov/news/2018/07/26/eac-commissioners-stress-importance-of-accessibility-and-security-in-joint-statement-commemorating-28th-anniversary-of-ada-/

Figure 1 - Key Components of the Electoral Process (source: Department of Homeland Security)

Scope

Consider, for instance, the thin boundaries of data security where personal data flows between social media platforms, commercial websites, and voting registration information (to name a few). Coupled with the dissemination of inaccurate media accounts (either "real" news dismissed as "fake news" or conversely "fake news" spread as fact), declining *public perception* of electoral security in its broadest sense including trust in the system, undermines management and integrity of the entire electoral process. Although these are all important aspects pertinent to the security of elections, they are beyond the scope of the proposed first level (voting process) and merit a separate, specific detailed analysis.

Conceptual aspects of security

With regards to the *conceptual aspects of security*, traditionally, election security has focused on encryption, digital signatures, protection of electoral stakeholders, voting information, facilities, and events. According to the EAC**,** *Cybersecurity* is 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 wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems.[10]" As a result, a common misconception is that **hackable voting technology,** broadly defined, is the weakest link in the election process. For instance, there are range of opinions as to whether ballot scanners are better or not in terms of security when compared to touchscreen-based voting. However, in reality, the most problematic security problems come not from hardware technology design per se, but from software bugs, or errors in processes, which requires a different approach to addressing problems. Regardless of the initial arguable conceptual pros and cons regarding ballot scanners and touchscreen-based voting, the main security concerns result from systems that were designed and implemented without a sufficiently comprehensive definition of security, in all its dimensions.

Level

In terms of *level of system*, election officials in all jurisdictions, regardless of size, need to assess and secure the electoral process at each level, not only assessing the technology but also intermediary government functions that connect directly to it, such as handling and operation of the voting workflow; as well as external functions that touch the entirety of the elections process: procurement, staffing, and vendor management. This underscores the importance of thinking about security not simply at the physical and technology/access level, but more comprehensively in terms of integrity of the entire voting process.

Associated concerns

In terms of *associated concerns*, findings from the recent 2018 National Academies of Sciences, Engineering, and Medicine report, *Securing the Vote: Protecting American Democracy* observed: "There are numerous ways in which the integrity of elections can be affected. Election results may be improperly tallied or reported. Inaccuracies may be introduced by human error or because of a lack of proper oversight. Election tallies and reporting may also be affected by malicious actors. […] Information on voting locations, voting times, and voting processes may be manipulated to mislead potential voters.

[10] Source: 2009 National Infrastructure Protection Plan (NIPP). (2009). DHS https://www.dhs.gov/publication/nipp-2009-partnering-enhance-protection-resiliency

Registration data may be altered to disenfranchise voters. Counting errors may affect manual or electronic tallying methods. Tallies may be inaccurately reported because of carelessness or malicious activity. After the primary reporting of results, evidence that enables verification of the reported results may be altered or destroyed." We believe then, that development of rational, comprehensive approaches to assess security, are called for, rather than falling back on simple, "default" approaches like paper ballots and scanners being the optimal security solution, while overlooking all of the other, less discussed, ways that security of the voting process can be compromised.

This paper proposes an approach, an innovative assessment framework, including a comprehensive, independently defined, end-to-end voting systems security model (General Model for Voting System Security (GMVS)). This alternative to a more traditional approach focused solely on physical *voting security*; is based on a more expansive objective of *overall* election integrity. Such a systems-based, multifactor approach not only monitors and assesses the various security failure points but has a wider scope that addresses other factors in the electoral process that include the issues of privacy, ability to participate (e.g. accessibility and usability considerations) as well as transparency, and confidence in the electoral institutions. We argue that disruption to the integrity of voting can be minimized by coupling cybersecurity approaches to a comprehensive multi-level security and threat reduction strategy.

Security policy

With regard to *security policy issues, barriers, and opportunities*, and other critical regulations affecting system design, we note that policy and regulation tend to be developed in a reactive manner in the U.S., frequently in response to technological advances and events which draw public awareness. The movement away from hand-counted paper ballots and older mechanical technologies was already occurring by 2000, in favor of a growth in optical scanners and electronic voting technologies such as DREs. In an effort to address issues raised by the Florida recount problems of 2000, Congress passed the Help American Vote Act (HAVA) in 2002, which banned the use of lever machines and punch cards in federal elections, and also required that all precincts have at least one voting machine accessible to voters with disabilities (MEDSL). HAVA also mandated the scope in which the Election Assistance Commission (EAC) may test and certify voting equipment, and administer a national clearinghouse on elections that includes shared practices, information for voters and other resources to improve federal elections. EAC is also charged with developing guidance to meet HAVA requirements, and developing and adopting the Voluntary Voting System Guidelines (VVSG).

Moreover, Congress again recognized the need to focus on election integrity, and in March, 2018, appropriated $380 million in election security grants made available to all 50 states, the District of Columbia, Puerto Rico, Guam, American Samoa and the U.S. Virgin Islands, to improve administration of elections for federal office, including to enhance election technology and make election security improvements under certain conditions.

While efforts toward addressing security of the electoral system are being made, such as VVSG 1.1 (the current version), the $380 million in Congressional funding, and other measures taken at the state level, are beneficial in terms of improving the security of our systems, they still fall short in desired outcome. A system compliant with VVSG 1.1 still is not necessarily a totally secure system, in that the focus of VVSG 1.1 is not *primarily* security, and provision of (Federal) resources only addresses part of the problem. That said, these are laudable advances, but not enough. An alternative, such as allowing jurisdictions to adopt innovative security approaches could add to the options available.

Communication and public outreach

With regard to the role of *communication and public outreach*, in addressing security concerns, and to facilitate collaborative/partnership activities with other targeted constituencies, the CSIS (2018) notes that while campaigns and election night reporting systems "cannot be used to directly disrupt or manipulate elections, attacks on these systems pose a serious threat to public confidence in American democracy." This underscores the importance of a robust communications and outreach/engagement strategy. This includes:

1. development of ongoing outreach and engagement with key stakeholders, as well as a focus on vulnerable populations;
2. monitoring current events and changes in best practices in the area of social as well as traditional media platforms;
3. developing a multiple-platform strategy for constituent engagement;
4. establish ongoing collaboration with other local and state election officials, and;
5. develop an election voting incident plan that helps election officials prepare and train for, and test responses ahead of time.

The Belfer Center (2018) suggests components of the plan include: cataloguing Incident Best Practices, a communications process workflow, response checklist, and scenario planning and dry runs.

4.0 Critical System Approaches: Assessment and election audit/evaluation tools

Technology, voting processes, and overall election management are key components that need to be subject to security and risk assessment (Darnolf, 2018) on the front-end, as well as ongoing monitoring and audits during and post-election (NASEM, 2018). In this regard, it is useful to step back and consider the entire election cycle (see Figure 1 above), as a set of points during which security checkpoints can occur. Ensuring effective election security ideally involves implementing a set of proactive processes. First of these is to map out strategic objectives and outcomes built upon a set of assessment and auditing practices. A very useful straightforward tool, for example, was developed by the Elections Center – the Elections Security Checklist (see Appendix 2). Coupled with the development of more in-depth background briefs, best practices (both in the U.S. and globally) and sample implementation cases, this sort of list could be an important component of an election's security toolbox. However, it is yet short from helping us achieve a comprehensive assessment on election integrity. Other similar tools have been proposed:

- Elections Security Checklist. (Elections Center, 2016).
- Checklist for Securing Voter Registration Data. (EAC, 2017)
- Securing the Nation's Voting Machines: A Toolkit for Advocates and Election Officials (Brennan Center, 2018)
- International IDEA's Electoral Risk Management Tool (ERM Tool)

Voting systems are complex distributed systems, with many potential points of failure. Voting systems must be correctly operated by many different persons with different levels of training, and they must be useable by the general public. They are targets of malicious actors who may have advanced technical capabilities, who may be well financed, and who may have strong incentives to tamper with the correct operation of the system.[11] Drawing on insights developed from a review of the baseline reference literature, we propose that any comprehensive approach to elections security be grounded in an empirical, fact-based discussion of not just physical security, but of the possible interaction effects of system level security variables, and ultimately aiming at voting system integrity as previously stated.

[11] Georgia Tech Research Institute, 2018, research in progress [https://iisp.gatech.edu/home]

An approach currently under development by Georgia Tech Research Institute is precisely aimed at tackling a comprehensive assessment of election integrity. The approach has two parts, a reference model and an analytic Independent Framework for Assessment (IFA).

The reference model (a work in progress) is called the *General Model for Voting Security (GMVS)*, and is designed to be a comprehensive reference to evaluate election integrity. It outlines a set of requirements that are described as “not an end unto themselves, but they are requirements that must be met to protect the primary voting system requirements in an adversarial model.” It basically outlines the aspects that a system must support in order to maximize its security.

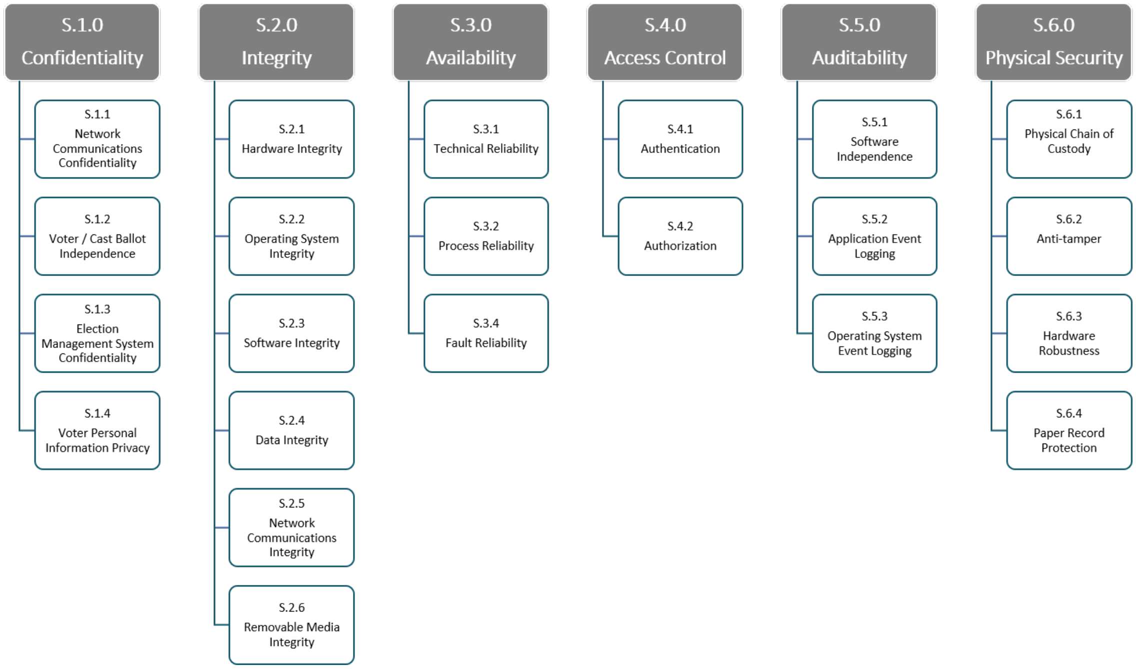

S.1.0 Confidentiality
S.1.1 Network Communications Confidentiality
S.1.2 Voter / Cast Ballot Independence
S.1.3 Election Management System Confidentiality
S.1.4 Voter Personal Information Privacy
S.2.0 Integrity
S.2.1 Hardware Integrity
S.2.2 Operating System Integrity
S.2.3 Software Integrity
S.2.4 Data Integrity
S.2.5 Network Communications Integrity
S.2.6 Removable Media Integrity
S.3.0 Availability
S.3.1 Technical Reliability
S.3.2 Process Reliability
S.3.4 Fault Reliability
S.4.0 Access Control
S.4.1 Authentication
S.4.2 Authorization
S.5.0 Auditability
S.5.1 Software Independence
S.5.2 Application Event Logging
S.5.3 Operating System Event Logging
S.6.0 Physical Security
S.6.1 Physical Chain of Custody
S.6.2 Anti-tamper
S.6.3 Hardware Robustness
S.6.4 Paper Record Protection

Figure 2 - *General Model for Voting Security (GMVS)*

In addition to the GMVS, an analytic framework (IAF) outlines how the process of assessment could best be conducted, independently, in order to evaluate security early on from the design phase. The framework assumes that an independent agent (in yellow, below) will provide the reference for the assessment (the GMVS in this case) and that agent will assess security first at design, then at implementation, and then at production:

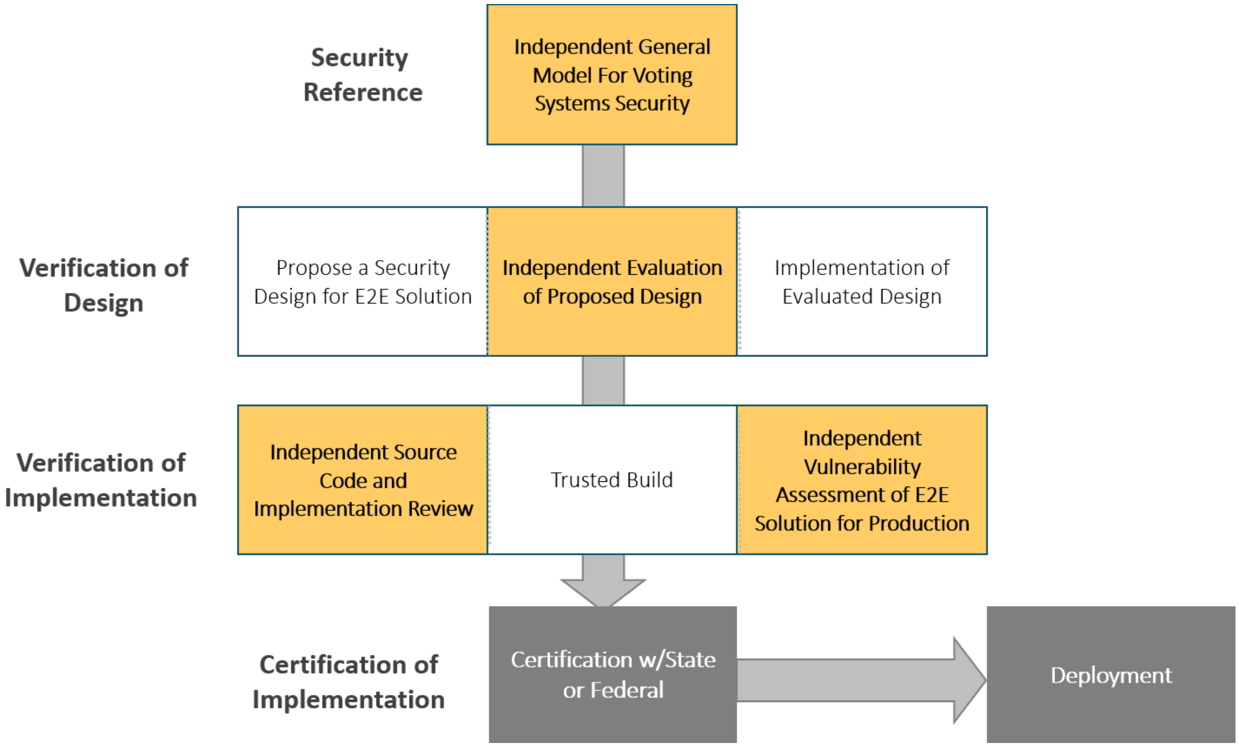

Security Reference
Independent General Model For Voting Systems Security
Verification of Design
Propose a Security Design for E2E Solution
Independent Evaluation of Proposed Design
Implementation of Evaluated Design
Verification of Implementation
Independent Source Code and Implementation Review
Trusted Build
Independent Vulnerability Assessment of E2E Solution for Production
Certification of Implementation
Certification w/State or Federal
Deployment

Figure 3 – ***Analytic Framework for Assessment (Independent Assessment Framework)***

The approach as outlined above, is based on a 1. requirements component, 2. a threat component, and 3. security component, detailed below.

1. The **Requirements** component includes requirements for a general voting system and is weighted toward factors particularly impacted by security – of the physical components as well as the overall electoral process. Additional elements include the need for voting equipment to meet federal, state, and local system standards and requirements (including accessibility and usability objectives), cost to *acquire* new equipment and availability of funding, ability to maintain equipment and timely vendor support, and more strategic considerations, such as overall performance/features including usability and longevity of voting equipment.
2. The **Threats** component is a systematic description of the ways that an attacker could attack a system. Many of the threats to an electronic voting system will be common to any complex computing system, however some of the threats to a given electronic voting system are particular to that system. That said, threat models are just that – models, and serve to reduce risk and uncertainty, but are not completely unassailable. Part of the difficulty in creating a secure system is that not all threats can be anticipated. Attackers may be clever and are not to be underestimated. Therefore, the importance of having a comprehensive threat model, with an end-to-end scope allows structural consideration of possible attacks against the system, and to build a protection model accordingly, based on layered defenses. If attackers devise ways to break one of them, other defenses can be called upon to mitigate further damage and will ultimately allow conduct an election with high confidence that the basic requirements are met. A good threat model does not only consider known particular vulnerabilities, but it attempts to anticipate general classes of threats known to computer security experts.

3. The **Security** component is a set of requirements that are derived from consideration of the general requirements of a voting system in an adversarial setting. The security requirements are a means to protecting an election, whereas the main requirements model is the end itself. In a perfect world, security requirements would be unnecessary (except perhaps to protect against routine failures and mistakes). As with other models in this work, the security model is neither totally inclusive nor absolute, but this security model is designed to serve as one basis for a meaningful protection model.

The benefit for electoral jurisdictions (and ultimately voters) of the proposed approach -- having a General Model for Voting Security, and using it as a reference within an independent assessment framework (IAF) -- is that it allows for the generation of a fairly complete and effective report of the security and integrity of a voting system solution, without having to invest vast amounts of money, time and resources:

- The independent generation of a comprehensive an end-to-end reference model to assess voting system security provides high assurance that most relevant aspects concerning security and integrity are going to be covered.
- Having a comprehensive reference is then about independently assessing voting systems based on that model.
- Since it is not particularly cost-effective for each jurisdiction in the country to perform such an assessment (as it will likely be redundant), we propose that each vendor submit their voting solution to a security assessment conducted by an independent, neutral third-party evaluator, significantly reducing the anticipated cost and time for jurisdictions.

Figure 4 (below) provides a conceptual illustration of the benefits of this approach.

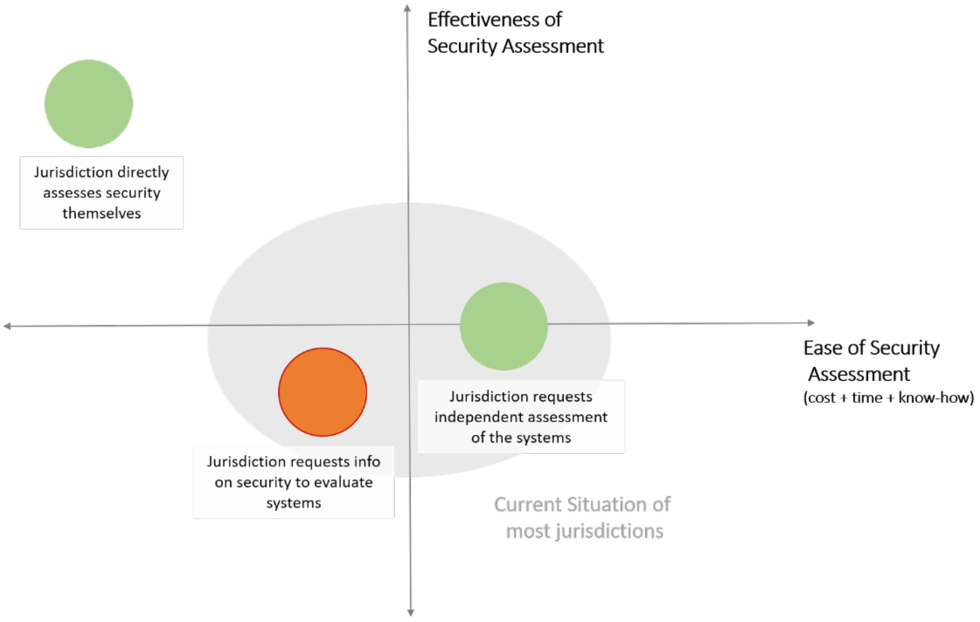

Effectiveness of
Security Assessment
Jurisdiction directly assesses security themselves
Ease of Security Assessment
(cost + time + know-how)
Jurisdiction requests independent assessment of the systems
Jurisdiction requests info on security to evaluate systems
Current Situation of most jurisdictions

Figure 4 General Model for Voting Security and Independent Assessment Framework Approach

The two axes capture dimensions of certainty (assurance of security) and implementation (capacities, complexity of implementation cost). Given the complexity and many aspects of security, how can a jurisdiction be sure that the various options actually account for, and provide the security needs of the local voting process? Jurisdictions, in this case, would need to have a sufficient understanding not just of the security factors, but also be able to monitor and validate that the systems are actually functioning as designed and deployed. The typical process would be to engage a security consultant to inform this process, but this also requires that jurisdictions be able ascertain the best fit consultant for the specific jurisdiction needs, as well as afford the consultant or the consultant's solutions.

In theory, following vigorous reviews of the current voting system and electoral practices, and hence, determination of key objectives, a jurisdiction issues requests to vendors for information on their systems (in this case, security focused) to initiate evaluation of their systems (depicted on lower left quadrant). This is the ideal approach. In practice, a lot of jurisdictions overwhelmed by the many concerns and demands of running elections, default to simply asking vendors to explain their security. This approach scores low on *Assurance of Security* axis, because vendors may not disclose security flaws of their systems to jurisdictions in their offers, and even if they do, it is not certain the extent to which vendors have done a comprehensive analysis themselves[12] This approach also scores low on the *Ease of Assurance* as it requires reading and understanding a security description that may not be standard, structured, and difficult to compare with other vendors' systems. This would support the rationale for standardized and consistent security descriptions and ideally, a comprehensive, understandable approach to security assessment and validation.

Jurisdictions also have a need for vendors to independently assess parts of their systems (middle right to the center quadrants). While a lot of jurisdictions are currently doing this, the requirements of this approach may result in less than desirable outcomes. For example, if the RFP states: "The vendor must provide an independent penetration test of its system" with no specific scope or approach defined, vendors may selectively do penetration testing in some parts of their systems to comply with the *stated* tender requirements. This means that the Assurance of Security dimensions is only increased to a minimum acceptable level (as at least some parts of the system have been independently assessed, and assuming that vendors make truthful efforts to include relevant parts in the evaluation) and a comprehensive assessment is not guaranteed. This condition is exacerbated by the reality that: 1) jurisdictions will "not pay" for assessment, specifically, 2) will not invest time as a required deliverable to tender, and likely will have access to executive summaries in these independent reports; 3) may simply rely on vendors statements that security is adequately provided for. As we have noted about, the sheer volume and complexity of elections related security material is overwhelming for specialists, more so for election officials juggling multiple priorities. This adds to an argument for a standardized, easily understood process of security assessment and validation.

Comprehensive system security assessment: The proposed model is one consisting of an independent external comprehensive security review. Under this approach, a jurisdiction requests that vendors independently assess their systems based on an E2E[13] independent model (Upper right corner). It scores high on the *Assurance of Security* dimensions, because an independent entity conducts the full E2E assessment of the system rather than a de minimis, set of selective penetration tests on *parts* of the system. Cost savings occur in several areas when required of the vendor during the procurement process and reduces demands on jurisdictions. This particularly makes sense if all jurisdictions follow this

[12] See for example, Balzarotti, et al. (2010); Ali & Murray (2016); Dunn & Merkle (2018)

[13] An end-to-end (E2E) verifiable voting system allows voters to: check that the system recorded their votes correctly, check that the system included their votes in the final tally, and. count the recorded votes and double-check the announced outcome of the election. (U.S. Vote Foundation).

standardized process, which has aggregated benefits by avoiding redundant independent assessments, hiring of consultants; and for vendors, this approach minimizes the need to have the same system to be evaluated multiple times with minor differences. If vendors do it once, the cost is "distributed" across all jurisdictions, and compliance with the independent assessment based on the same model, allows jurisdictions to easily compare options.

5.0 Innovation and New Approaches to Electoral Process Integrity

In this paper we have identified key security related issues/considerations facing elections officials and the general public, and propose an innovative system level model (**General Model for Voting System Security (GMVS**) that offers an approach that addresses these considerations and concerns. For non-experts or organizations with limited resources, an overall background can be obtained by reviewing current thinking on innovative approaches to security, and adopting customizable, targeted, issue-specific best practices and security and efficacy-based toolkits[14]. More broadly, developing a robust security approach (and hence integrity and confidence in) the electoral process can be enhanced by employing additional supporting tools, such as stakeholder outreach and development of collaborative efforts improve voting and election processes.

Addressing issues of security, at a minimum, requires a seeming full-time task of staying up to date on advances in IT and cybersecurity, developing assessment and lifecycle auditing and assessment plans before the election, during the election and after the election with appropriate tools and checklists. We argue, however that a more efficacious approach, applies the proposed assessment model, as part of developing a comprehensive, expansive view of the entire electoral process, including engagement with the various election stakeholders.

The central objective of the electoral process is to address the need for transparency and the transmission of reliable information to all stakeholders, which is a key rationale for an emphasis on security. Applying the three-pronged comprehensive voting integrity approach (Technology, Policy, Communication) then suggests that elections officials:

1. Regularly seek updates on cybersecurity from reliable sources.
2. Follow key sources on best practices for election management (including policy changes). While there are a number of sites that track information, it would be useful to have a library of guides and checklists that help elections stay on track. Other options include ongoing online training and self-assessment classes, and development of a set of hypothetical cases that can be explored in an interactive manner.
3. Utilize best practice approaches and toolkits both for outreach (communication) as well as soliciting input and engagement from key groups, which encourages participation and engagement.[15]
4. Considering the above, the model we have proposed - a General Model for Voting Security (GMVS) - addresses issues of security from a multilevel perspective and takes into account the interactive impacts of various aspects of security. The key underlying components of the model include the **Requirements component** for a general voting system, the **Threats component** is a systematic description of the ways that an attacker may attack a system at all levels and the **Security component,** which designs specific approaches and mitigation to avoid interference and protect the integrity of the voting process.

[14] See for instance: Belfer Center (The State and Local Election Cybersecurity Playbook, (2018); Elections Center, (2016).

[15] e.g. Agawu, E. A. (2018)

- Requirements (planning/scope/considerations)
- Threats (including assessment and audits)
- Security consists of the application of tools, check list and best practices, and the ongoing commitment to keep up not only with technological advances, but also best practices and changes in the social and communication environments

In summary, we propose that jurisdictions explore adoption of a standardized approach such as the **General Model for Voting System Security (GMVS) & Independent Assessment Framework (IAF)** (currently under finalization) or similar such approach. The model addresses dimensions of certainty (assurance of security) and implementation (capacities, complexity of implementation cost) as a way of navigating the complexity of election security. Advantages of this approach include reduction of uncertainty due to the rapidly change technology and security landscape, cost savings to jurisdiction from simplified (and more assured) procurement specification, assessment and evaluation, and to vendors from having to repeatedly conduct security audits which may differ minimally from local to local, but which require redundant efforts to address. Overall, the ultimate benefit is to all stakeholders by potentially reducing one aspect of security uncertainty, while at the same time achieving cost-savings and increased public perception of election system integrity.

Appendix 1

The National Academies Committee on the Future of Voting: Accessible, Reliable, Verifiable Technology, produced the following cybersecurity recommendations (Summary." National Academies of Sciences, Engineering, and Medicine. 2018. Securing the Vote: Protecting American Democracy. Washington, DC: The National Academies Press. doi: 10.17226/25120) focused on the importance of the auditing aspect:

Election Auditing

5.5 Each state should require a comprehensive system of post-election audits of processes and outcomes. These audits should be conducted by election officials in a transparent manner, with as much observation by the public as is feasible, up to limits imposed to ensure voter privacy.

5.6 Jurisdictions should conduct audits of voting technology and processes (for voter registration, ballot preparation, voting, election reporting, etc.) after each election. Privacy-protected audit data should be made publicly available to permit others to replicate audit results.

5.7 Audits of election outcomes should include manual examination of statistically appropriate samples of paper ballots cast.

5.8 States should mandate risk-limiting audits prior to the certification of election results.[12] With current technology, this requires the use of paper ballots. States and local jurisdictions should implement risk-limiting audits within a decade. They should begin with pilot programs and work toward full implementation. Risk-limiting audits should be conducted for all federal and state election contests, and for local contests where feasible.

5.9 State and local jurisdictions purchasing election systems should ensure that the systems will support cost-effective risk-limiting audits.

5.10 State and local jurisdictions should conduct and assess pilots of end-to-end-verifiable election systems in elections using paper ballots.

Appendix 2

One list of best practices, developed by the Belfer Center (The State and Local Election Cybersecurity Playbook, 2018) include:

- Create a proactive security culture. Risk mitigation starts with strong leaders who encourage staff
- Treat elections as an interconnected system. Adversaries can target not only individual parts of the elections process but also the connections between them.
- Have a paper vote record.
- Use audits to show transparency and maintain trust in the elections process.
- Implement strong passwords and two-factor authentication.
- Control and actively manage access. Everyone with access to the computer network can become a target and often only one target needs to be compromised for an attack to succeed.
- Prioritize and isolate sensitive data and systems. Risk is where threats and vulnerabilities meet. To reduce risk, officials need to think about what vulnerabilities will cause the most damage, given the threat environment. Officials consider two things when making a risk assessment: (1) what data is most sensitive and (2) what disruption could be most damaging to voters' trust in the election.
- Monitor, log, and back up data.
- Require vendors to make security a priority.
- Build public trust and prepare for information operations. Communication is the cornerstone of public trust. Transparency and open communication will counter information operations that seek to cast doubt over the integrity of the election system.

References

Ali, S. T., & Murray, J. (2016). An overview of end-to-end verifiable voting systems. *Real-world electronic voting: Design, analysis and deployment*, 171-218.

lvarez, R. M., Levin, I., & Li, Y. (2018). Fraud, convenience, and e-voting: how voting experience shapes opinions about voting technology. *Journal of Information Technology & Politics*, *15*(2), 94-105.

Agawu, E. A. (2018). *How To Think About Election Cybersecurity*. New America Foundation. https://www.newamerica.org/cybersecurity-initiative/policy-papers/how-to-think-about-election-cybersecurity/

Augoye, V., & Tomlinson, A. (2018). Analysis Of Electronic Voting Schemes In The Real World. *Analysis*. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1013&context=ukais2018

Balzarotti, D., Banks, G., Cova, M., Felmetsger, V., Kemmerer, R., Robertson, W., ... & Vigna, G. (2010). An experience in testing the security of real-world electronic voting systems. *IEEE transactions on software engineering*, *36*(4), 453-473.

Belfer Center for Science and International Affairs, Harvard Kennedy School. (2018). "The State and Local Election Cybersecurity Playbook."https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

Brennan Center for Justice. (2018). Securing the Nation's Voting Machines: A Toolkit for Advocates and Election Officials. https://www.verifiedvoting.org/wp-content/uploads/2018/06/Securing-the-Nation-s-Voting-Machines-A-Toolkit-for-Advocates-and-Election-Officials.pdf

Brennan Center for Justice. (2015). America's Voting Machines at Risk. NYU School of Law. New York, NY. https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf

Byrne, M. (2017). Improving voting systems' user-friendliness, reliability, & security. *Behavioral Science & Policy*, 3(1), 14-24.

Center for Internet Security. (2018) et al., A Handbook for Elections Infrastructure Security, (East Greenbush, New York: Center for Internet Security, 2018), https://www.cisecurity.org/elections-resources/.

CSIS. (2018). *CSIS Election Cybersecurity Scorecard: The Outlook for 2018, 2020 and Beyond.* Washington D.C.: Center for Strategic and International Studies. https://www.csis.org/analysis/csis-election-cybersecurity-scorecard-outlook-2018-2020-and-beyond (October 29, 2018)

Counting Votes. (2012). Counting Votes 2012: A State by State Look at Election Preparedness. Report from Verified Voting, the Rutgers Law School Constitutional Litigation Clinic and Common Cause. Washington, D.C. Retrieved from: http://countingvotes.org/sites/default/files/CountingVotes2012_Final_August2012.pdf

Darnolf, S. (2018). Safeguarding Our Elections: Enhanced Electoral Integrity Planning. *SAIS Review of International Affairs*, *38*(1), 39-51.

DEFCON. (2017, September). DEFCON 25: Voting Machine Hacking Village – Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure. DEFCON. Retrieved from: https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf

Dunn, M., & Merkle, L. (2018, March). Overview of Software Security Issues in Direct-Recording Electronic Voting Machines. In *ICCWS 2018 13th International Conference on Cyber Warfare and Security* (p. 182). Academic Conferences and publishing limited.

Dzieduszycka-Suinat, S., Murray, J., Kiniry, J., Zimmerman, D., Wagner, D., Robinson, P., ... & Morina, S. (2015). The future of voting: end-to-end verifiable internet voting-specification and feasibility study. *US Vote Foundation*.

Election Assistance Commission (EAC). (2016). Ten Things Election Officials Can Do to Help Secure and Inspire Confidence in This Fall's Elections. Washington, D.C. Retrieved from: https://www.eac.gov/assets/1/28/EVN%20Top%20Ten%20v7.pdf

Election Assistance Commission (EAC). (2017). Checklist for Securing Voter Registration Data. https://www.eac.gov/assets/1/28/Checklist_Securing_VR_Data_FINAL_5.19.16.pdf

EAC (2017). Common Cybersecurity Terminology. https://www.eac.gov/documents/2017/09/21/common-cybersecurity-terminology/

Elections Center. (2016). Elections Security Checklist. https://www.electioncenter.org/election-security-infrastructure-elections-security-checklist.html

GAO. (2018). Elections: Observations on Voting Equipment Use and Replacement. Washington D.C.: Government Accountability Office. GAO-18-294: Published: Apr 11, 2018. https://www.gao.gov/products/GAO-18-294

Gonzalez, R. (2016, November). Google's Real-Time Map of Voter Issues is Totally Captivating. Retrieved from: https://www.wired.com/2016/11/googles-real-time-map-voter-issues-totally-captivating/

Governing Institute. (2016). *Understanding The Cyber Threat: A Policy Guide for Legislators* https://www.business.att.com/content/dam/attbusiness/briefs/industries-public-sector-policy-guide-brief.pdf

Harkins, R.; Kleiner, A.; & Pinter, J. (2018). *From Policy to Practice: Strengthening Cybersecurity in State Governments*. Microsoft White Paper. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2om9h

Hsu, J., & Bronson, G. (2018). E-Voting Technologies Usability: A Critical Element for Enabling Successful Elections. In *Emerging Challenges in Business, Optimization, Technology, and Industry* (pp. 61-78). Springer, Cham. https://link.springer.com/chapter/10.1007/978-3-319-58589-5_5

International Institute for Democracy and Electoral Assistance (IDEA). (2013). Electoral Risk Management Tool (ERM Tool) https://www.idea.int/sites/default/files/tools/Overview-Electoral-Risk-Management-Tool.pdf

Miller, D.T. (2018) "Cyber Interference in Elections and Federal Agency Action*." Harvard Law Review Blog.* OCTOBER 29, 2018. https://blog.harvardlawreview.org/cyber-interference-in-elections-and-federal-agency-action/

McCaig, A. (2017, August). Successful voting systems must be accurate, usable, accessible and secure. Rice University, Houston, TX. Retrieved from: http://news.rice.edu/2017/08/15/successful-voting-systems-must-be-accurate-usable-accessible-and-secure/

MIT Election Data and Science Lab (MEDSL). *Voting Technology*. https://electionlab.mit.edu/research/voting-technology

National Academies of Sciences, Engineering, and Medicine (NASEM). (2018). *Securing the Vote: Protecting American Democracy.* Washington, DC: The National Academies Press. doi: https://doi.org/10.17226/25120.

NCSL. (2018). *Voting System Standards, Testing and Certification.* National Conference of State Legislatures. http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx

Norden, L. (2015). Cybersecurity: Ensuring the Integrity of the Ballot Box. Report by the Committee on House Oversight and Government Reform, Subcommittee on Information Technology. Washington, D.C. Retrieved from: https://oversight.house.gov/wp-content/uploads/2016/09/2016-09-28-Norden-NYU-Testimony.pdf

Norden, L., & Famighetti, C. (2015, September). America's Voting Technology Crisis. The Atlantic. Retrieved from: https://www.theatlantic.com/politics/archive/2015/09/americas-voting-technology-crisis/405262/

National Conference of State Legislatures. (2015). Voting Equipment. Washington, D.C. Retrieved on: http://www.ncsl.org/research/elections-and-campaigns/voting-equipment.aspx

National Conference of State Legislatures. (2018). Voting System Standards, Testing and Certification. http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx

Norris, P., Wynter, T., & Cameron, S. (2018). Electoral Integrity & Campaign Media. 2018 MID-YEAR UPDATE. Electoral Integrity Project. https://www.electoralintegrityproject.com/2018midyearupdate/

Pew Charitable Trusts. (2016). Aging Voting Machines Cost Local, State Governments. Washington, D.C. Retrieved from: http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2016/03/02/aging-voting-machines-cost-local-state-governments

Pew Research Center. (2016b). Top Issues in 2016 Election. Washington, D.C. Retrieved from: http://www.people-press.org/2016/07/07/4-top-voting-issues-in-2016-election/

Pew Research Center. (2017). Q&A: Pew Research Center's president on key issues in U.S. polling. Washington, D.C. Retrieved from: http://www.pewresearch.org/fact-tank/2017/06/16/qa-pew-research-centers-president-on-key-issues-in-u-s-polling/

Rid, T., & Buchanan, B. (2018). Hacking Democracy. *SAIS Review of International Affairs*, *38*(1), 3-16.

Warkentin, M., Sharma, S., Gefen, D., Rose, G. M., & Pavlou, P. (2018). Social identity and trust in internet-based voting adoption. *Government Information Quarterly*, *35*(2), 195-209.

Tuttle, H. (2018) "Hack the Vote 2: Cyberrisks to Election Infrastructure." *Risk Management*. (October 1, 2018). http://www.rmmagazine.com/2018/10/01/hack-the-vote-2-cyberrisks-to-election-infrastructure/

U.S. House Committee on Oversight and Government Reform, Cybersecurity of Voting Machines: Hearing before the Subcommittee on Information Technology, 115th Cong., 1st sess. (November 29, 2017), available at https://oversight.house.gov/hearing/cybersecurity-voting-machines/

University of Pennsylvania, Wharton School Public Policy Initiative. (2016). "The Business of Voting: Market Structure and Innovation in the Election Technology Industry." https://publicpolicy.wharton.upenn.edu/business-of-voting/

Verified Voting. (2017). Voting Equipment in the United States. Retrieved from: https://www.verifiedvoting.org/resources/voting-equipment/

Weiser, W. R., & Opsal, E. (2014). *The state of voting in 2014*. Brennan Center for Justice at New York University School of Law.