Election Laws Position Update
Part 1

Election Laws Study Committee:

Rona Ackerman (Editor), Pamela Berg, Janet Boyd, Allison Brown, Judy Collins, Virginia Cowles, Mary Crutchfield, Marianne Feeney, Shelley Gelbert, Lisa Koteen Gerchick, Evelyn Glazier, Sidney Johnson, Rebecca Lawson, Robin Marcato, Susan Mulnix, Jane Newell, Linda Rice, Anne Sterling, Anna Weber.

Steering Committee for Part 1: Allison Brown, Lisa Koteen Gerchick, Sidney Johnson, Jane Newell

May 1, 2020

Election Laws Position Update: Part I

Table of Contents — Page Reference in the Report

Introduction

Although state League members are covered by national positions, the League of Women Voters of Virginia (LWV-VA) wants to articulate its own Election Laws positions more clearly to assure they fully cover advocacy on issues that may come up. LWV-VA members voted at Convention 2019 to review and update the following items in the LWV-VA Election Laws position:

A. Include election processes, laws, and regulations (e.g. post-election audits) that ensure free and fair election results, transparency, security and accountability
B. Prepare amendment to State position to strengthen support for security, including physical security of voting equipment and ballots
C. Review the language supporting electronic voting
D. Add a statement opposing requirement for photo ID at polls
E. Consider and explore the effectiveness and impact of ranked choice voting
F. Address voter suppression

This will be done in two parts—Part 1 (topics A-D) in 2020 and Part 2 (topics E-F) in 2021. At the 2020 National Convention, the League of Women Voters of the United States (LWVUS) will consider the proposal, "Concurrence on Voter Representation/Election Processes (Electoral Systems)".[1] If passed, its impact will be discussed in Part 2.

LWVUS publishes its position on elections in the Representative Government section of *Impact on Issues, 2018-2020*.[2] The League of Women Voters of Virginia (LWV-VA) publishes its position in the Election Laws section of *Positioned for Action, 2019.*[3] In the discussion that follows, we have provided relevant excerpts from these positions. Fuller descriptions can be found in found in Appendix A or the source publications.

Part A: Include Election Processes, Laws, and Regulations (e.g. Post-Election Audits) That Ensure Free and Fair Election Results, Transparency, Security, and Accountability.

A1. A Concise Statement to the Point That Our Democratic System Depends on Voters' Faith in the Integrity of Election Processes and Election Outcomes

Voters have a right to be confident in the integrity of the election process. Election integrity means that every step of the voting process is trustworthy; that individual votes are secure, confidential, and counted accurately; and that ultimate outcomes are free from any outside interference. Election systems, from voter registration through the whole sequence of voting activities and certification, are vulnerable to the extent that they rely on electronic means to operate, need protection for equipment and materials, and require well-trained personnel. The Senate Intelligence Committee reports on Russian attempts to interfere with our election processes show that concerns about the hackability of our systems are justified.[4] Virginia was identified as one of the states on which hacking was attempted, but unsuccessfully.[5]

Study Committee Recommendation

The study committee recommends modifying the current Election Laws Position in Brief to include the addition of the wording in italics below.

Position in Brief: The League of Women Voters of Virginia believes that democratic government depends on the informed and active participation of its citizens; that voting is a right and responsibility; and that election laws, regulations and administrative procedures should be uniformly designed and applied, and adequately funded to facilitate and increase voter participation throughout

Virginia.[6] *The League further believes that continuous monitoring and upgrading of security, to address both cyber- and physical threats to all components of the elections system and process, ensures that the citizens can trust the integrity and outcomes of elections.*

A2. Adoption and Maintenance of Certification Standards and Recertification if Needed to Meet or Exceed Federally Set National Standards

Background

The first Voluntary Voting System Standards were issued by the Federal Election Commission in 1990. The standards addressed factors of security, functionality, privacy, usability, and accessibility. After the passage of the Help America Vote Act (HAVA) in 2002, an independent testing authority was created to assess devices against an updated body of standards, the Voluntary Voting System Guidelines (VVSG) 1.0. In 2006, HAVA transferred certification authority to the Election Assistance Commission (EAC).[7] During the next 10 years, EAC made only minor changes to VVSG, releasing version 1.1 in 2015.[8] EAC and National Institutes of Standards and Technology (NIST) have started working on VVSG 2.0,[9] designed to separate the principles and guidelines for standards (requiring approval by EAC) from the detailed technical testing requirements. The intention is to allow the implementation of certification to be dynamic over time, to adopt recognized standards from external agencies, and to ensure that technical details are approved by technical experts rather than by political appointees.[10]

The EAC's Technical Guidelines Development Committee, with support from NIST, develops an initial set of recommendations for each VVSG iteration. Those recommendations must be approved by EAC after a public comment period. NIST recommends Voting System Test Laboratories (VSTLs) for accreditation by EAC. EAC certifies voting equipment that is in compliance with the guidelines.[11]

VVSG 1.1, the current version, has requirements including functionality, usability and accessibility, hardware, software, telecommunications, security, quality assurance and configuration management. Cybersecurity-related requirements overlap several of these categories. The guidelines specify the collection of data to support post-election tabulation audits and include a review of source code for best programming practices.

VVSG 2.0, approved in principle but lacking testing specifications, reorganizes the requirements into fifteen principles, of which five are related to security: auditability, ballot secrecy, access control, physical security, data protection, system integrity, and detection and monitoring. The last two introduce new requirements to address security risks. Other important updates strengthen criteria for encryption and authorization.[12,13]

The greatest weaknesses of the current certification process are the inflexibility of the testing process and the unreasonable amount of time required to approve updates to the standards. These problems are compounded by lack of continuity at the leadership level at the EAC. Considering that new cyberthreats appear every 24 hours, a federal certification standard that takes 10 years to update is unacceptable. A nimbler approach to implementation of testing may be possible under VVSG 2.0.

Current Status of Certification in Virginia

The voting systems in Virginia must meet requirements specified in the Code of Virginia.[14] After receiving EAC certification, voting machine manufacturers (vendors) may apply for Virginia certification by submitting a Technical Data Package. A VSTL conducts testing according to Virginia standards. After certification, the Virginia Department of Elections (ELECT) requires that local election officers test all devices prior to accepting them for use. ELECT will supervise a test use of systems in an actual election prior to final certification.[15]

Virginia's standards build on federal standards by adding state-specific corporate, operational, and security standards.[16] Periodic updates can leverage existing standards that have been adopted by other government agencies concerned with cybersecurity, as well as best practices in election security. Virginia requires that vendors report and take action on security or operational failures, or risk decertification. The

standards also include numerous requirements for creating and securing an audit trail of device and manual activities. Such data are an essential component of post-election audits.[17]

Most certifications have been conducted under the 2015 Virginia standards, but a handful have been grandfathered after assessment by ELECT. It is expected that all devices will need to meet the September 2019 standards in the very near future.[18] The new standards state that the State Board of Elections (SBE) "reserves the right to require recertification when new VVSG guidelines or changes to regulations and/or standards occur."[19] Decertification can result from reported security or performance failures, the vendor's failure to meet certain corporate standards, or at the stated end of life for the hardware or software.[20]

Virginia also defines standards for approval of electronic pollbooks (EPBs) placed in use after May 1, 2014. The SBE adopted new standards in December 2019. The proposed standards strengthen security for cloud connectivity of EPBs that would support their use in vote centers.[21] These new standards put Virginia in the forefront of election security for EPBs; the federal government does not have such standards yet (see p. 11).

Current LWVUS and LWV-VA Positions

LWVUS: Leagues should also consult standards developed by the Election Assistance Commission (EAC) pertaining to voting systems when studying or improving their own voting systems.[22]

LWV-VA: No position on standards for voting systems.

Study Committee Recommendation

The study committee recommends that the LWV-VA Election Laws position be modified to support standards and a robust certification process for election systems including

- Updating certification standards regularly to keep pace with the state of knowledge of the cybersecurity landscape
- Ensuring localities have sufficient resources, both expertise and financial, to manage updates to voting systems as certification standards evolve
- Requiring standards for security practices of voting machine vendors, their personnel and consultants/contractors
- Mandating state certification for all components of election management systems
- Recommending that the Commonwealth coordinate with other states in devising and implementing certification regimes

A3. Management of In Person Absentee Voting, Particularly in Light of New No Excuse Absentee Voting Provision

Except when specifically referencing the current Virginia law, which is termed no excuse absentee voting (NEAV), this report will use the term early voting.

Background

The Brennan Center for Justice (Brennan Center) issued a report in 2013 that recommended that all states and local jurisdictions implement the following early voting policies to expand the benefits of early voting nationwide:

- Begin early in person voting two weeks before Election Day;
- Provide weekend voting, including during the weekend before Election Day;
- Set minimum daily hours for early voting and provide extended hours outside standard business hours;
- Allow use of both private and public facilities;
- Distribute early voting places fairly and equitably;

- Update poll books daily; and
- Educate the electorate about early voting.[23]

The bipartisan Commission on Election Administration (precursor of the EAC) released a report in 2014 endorsing early voting.[24] While urging states to expand early voting, the Commission also cautioned states not to simultaneously expand early voting and excessively reduce the resources available for Election Day.[25] In 2014, early voting states, on average, provided 19 days for voting.[26] The report also summarizes the objections heard to early voting, including the different levels of information about the candidates, additional staffing by election officials and campaigns, lost and delayed mailed ballots, and greater risk of fraud.[27]

The National Conference of State Legislatures has done extensive work on early voting processes, as 41 states have statutes allowing some form of no excuse absentee voting.[28] Research by the Virginia Public Access Project indicates considerable and growing interest by Virginia voters in voting early.[29]

LWV-Fairfax Area released a statement in 2018 supporting no excuse absentee voting for both mail and in person, based on the following reasons:

- All voters should have equal access to the ballot.
- No voter should have to provide personal unrelated information to cast a ballot.
- Voters have experienced confusion about their eligibility to vote before Election Day.
- Voting absentee in person is as secure as voting on Election Day.
- Local Election Offices have had success in reducing long lines on Election Day by encouraging absentee voting.
- For voting absentee in person, eliminating the cumbersome process of completing the absentee application would save time as well as the expense of printing the form.
- Extra personnel are needed to explain the form and check it for completion before a voter can proceed to checking in.
- Eliminating the use of the application form would speed the voting process considerably.

The Fairfax Area League also indicated their belief that the costs would be a wash, with gradual decrease of voters on Election Day at the polls.[30]

Early Voting in Virginia

Effective for the November 2020 General Election, Virginia law now allows any registered voter to vote by absentee ballot in person or by mail beginning 45 days before election day, without any excuse. This changes the 2019 rule that would have allowed in-person only voting, beginning on the second Saturday immediately preceding any election in which the voter is qualified to vote, without providing a reason or making prior application for an absentee ballot.[31] The 45-day rule was passed by the 2020 General Assembly ,[32] and was signed by the Governor. The 2020 General Assembly, with the Governor's signature, also approved allowing voters to be added to a permanent list of absentee voters who will be sent an absentee ballot for mail-in voting.[33]

The 2020 General Assembly changes in large part reflect the SBE endorsed early voting recommendations included in an 2019 ELECT report[34] This report, prepared before the 2020 Session, addresses various issues that were predicted to arise due to the more limited 2019 expanded absentee voting rule that only permitted no-excuse absentee voting for in-person voters. However, the new full 45-day early voting period that will go into effect in November 2020 has similar challenges, including the need to add voting centers, election security, and other enhancements. The following chart describes the various SBE-endorsed legislative proposals.

Bill Topic	Summary
Technical Changes	• For special elections, absentee voting in person shall be available as soon after the deadline in the Code §24.2-701.1(a) as possible.[35] • Absentee ballot applications may be completed either at the general registrar's office or at any of the additional locations for absentee voting.[36]
Voting Centers	• Clarifies that any applicant who is in line to cast his ballot when a voting center closes shall be permitted to cast his ballot on that day. • Shifts the ability to establish voting centers from county or city electoral boards to the governing body of each county and city, by ordinance. • Establishes notice requirements for general registrars when voting centers are established or changed. • Makes voting centers equivalent to the office of the general registrar for the purposes of completing an absentee ballot application in person. • Clarifies the requirements concerning distributing campaign materials during the absentee voting period, with reference to Virginia Code § 24.2-604. (Prohibited activities at polls; notice of prohibited area; electioneering; presence of representative of parties or candidates; simulated elections; observers; news media; penalties).[37]
Timeframe Eligibility	• Replaces excuse-based absentee voting with a full 45-day period of no excuse absentee voting.[38]

ELECT is proposing to give local registrars flexibility in implementing the new early voting 45-day period. Christopher Piper, Commissioner of Elections in Virginia, is particularly sensitive about not imposing unfunded mandates on localities tasked to implement the new requirements; however, he believes ELECT can be helpful in providing voluntary standards and guidance (e.g., for pollbooks used by satellite or early voting centers).[39]

Registrars' Perspectives

Allison Robbins, Registrar, Wise County and current president of the Voting Registrars Association of Virginia (VRAV), supports the full 45-day early voting period. VRAV does not have a position on early voting, but Ms. Robbins believes that members are generally supportive.[40]

Gretchen Reinemeyer, Registrar, Arlington County, supports complete removal of an excuse requirement for both in person and mailed ballots for the entire 45 days. She believes it could be implemented at no additional cost beyond what is required for the one week, no excuse absentee voting period under current law. She does not anticipate having to open the early voting centers more than two weeks prior to the election if a 45-day early voting period is established.[41]

Walt Latham, Registrar, York County, believes that the switch to no excuse absentee voting can be done. However, he is concerned about budget impacts and not giving localities enough time to implement the changes. Mr. Latham believes that the localities are less well prepared to handle mailed ballots than in person voting because of the necessity of deciding how to mass print and mail the ballots. He believes that Virginia should set standard rules on minimum levels of service for early in person voting locations, in order to ensure equal access and uniformity of implementation.[42]

Dianna Moorman, James City County Registrar, is concerned primarily about early voting by mail. Her office already struggles with the seven-day deadline. By law, they currently have three days to mail the ballot to the voter. The ballot then has to travel to the voter, the voter has to complete it, and then mail it back to the registrar's office, all within seven days. She would like some restrictions so that voters are not able to request that ballots be mailed to them, for example, three days prior to an election, which simply is not possible due to logistics. Having no timeline at the end of the voting cycle will set up the registrar's office to fail.[43]

Current LWVUS and LWV-VA Positions

LWVUS: Since 2013, LWVUS has promoted five key proactive election reform priorities, one of which is the expansion of early voting.[44]

LWV-VA: Supports legislation to allow all registered voters to vote absentee without specifying a reason. Both choices–voting in person or by mail—should be offered.[45]

Study Committee Recommendation

The study committee recommends that the current LWV-VA Election Laws position on absentee voting be modified to include

- Adding *for the entire early voting period* to the current position on no excuse absentee voting, or early voting, for both in person and by mail voting
- Supporting the use of satellite vote centers to facilitate voter participation and give local registrars flexibility in implementing early voting in their localities, including determinations of locations and operational hours
- Recommending that the Commonwealth and localities to work together to ensure sufficient funding, staff, space, security, and access to accommodate any increase in voter participation

A4. Post-Election Audits

Background

First introduced in 2007,[46] risk-limiting audits (RLAs) are considered the gold standard of post-election audits.[47] To conduct an RLA, the election must be conducted using a voter-verified paper trail. An RLA provides strong statistical evidence that the outcome of an election is right and has a high probability of correcting an incorrect outcome.[48] A random sampling of cast ballots is audited right after an election and before the election is certified, limiting the risk that the outcome was wrong. In a nutshell, election officials compare randomly selected sample batches of cast ballots to the machine counts generated during the election. The sample size is determined in part by the apparent margin of victory in the contest: the wider the margin, the smaller the sample has to be. If examination shows a result that matches perfectly or within a predetermined margin of error, the audit can stop, and the election results are certified. If the results do not correlate, the sample size must be increased. If the comparisons continue to indicate that the outcome was in error despite ever-larger samples, the audit could end in a full recount. The election cannot be certified until the RLA has ended. In this way, not only is the election audited in a cost-effective way to ensure that the result is accurate but, if the result is wrong, the audit corrects the error.[49]

Nationally, the interest in post-election audits, including risk-limiting audits, has grown.[50] In 2010, the EAC provided grants to "support research, development, documentation and dissemination of a range of procedures and processes for managing and conducting high-quality logic and accuracy testing and post-election audit activities. California, Colorado, and Ohio used the awarded grant money to conduct research on RLAs, and from 2008 until present, RLA pilots have been conducted in jurisdictions in California, Colorado, Indiana, Ohio, and Virginia."[51]

In 2019, Nevada enacted an election security law that includes phasing in risk-limiting audits; Georgia will pilot an RLA in 2021.[52] Seven states have told the EAC that they will use 2018 federal funds for post-election audits: Alabama, Colorado, Connecticut, Kansas, Minnesota, Mississippi, and Vermont (additional states will use the funds for audits, but did not specify post-election time periods).[53]

Organizations that advocate for election security have long promoted the application of RLAs.[54] In 2018, the National Academies of Sciences, Engineering, and Medicine (NAS) recommended that "States…mandate risk-limiting audits prior to the certification of election results….Risk-limiting audits should be conducted for all federal and state election contests, and for local contests where feasible."[55] A strong consensus exists that post-election audits, preferably risk-limiting audits, are needed to protect elections and assure voters of the accuracy of those elections.

Current Virginia Law and Audits

Virginia requires a post-election risk-limiting audit, but the law only assesses the accuracy of the ballot scanner machines. Although the statute uses the term "risk-limiting audit," it does not satisfy the criteria for a "real" risk-limiting audit. The Code of Virginia (§24.2-671.1. Audits of ballot scanner machines.) provides for audits of election machines in every locality once every five years, but only after certification of the election's results. It specifies that the audit cannot affect the outcome of an election. Thus, it fails to meet three criteria of a "real" risk-limiting audit: that the audit is of ballots cast, that it is conducted before the election is certified, and that it has the potential to affect the outcome.

ELECT conducted eight pilot audits in 33 participating election board localities in 2019.[56] When presenting its report to the SBE, ELECT indicated that these audits "allowed ELECT to develop a process on how to administer the RLA pilot properly." Additionally, ELECT reported that "the remaining 99 localities would be randomly selected to determine when the audit should be conducted" and the audits would continue "once the RLA consultant contract is renewed" as the "contractors would help train ELECT staff to assist localities in administering the audits."[57] ELECT's report provided five recommendations and findings:

- The RLA process is manageable.
- Ballot storage may need to be adjusted.
- Investing in counting scales may be worthwhile.
- Auditing large contests is most efficient.
- Current statute poses certain challenges.

With regard to the statute's challenges, ELECT's report stated that the required random selections of localities to audit will present challenges as such selections would necessitate that only local contests conducted wholly within a single city or county be used. This criterion may be difficult to meet for many, if not most contests in Virginia.[58]

ELECT anticipates that the next steps are to conduct more audits, see how best to execute RLAs across Virginia, and then ultimately, to amend the law to institute post-election, pre-certification audits of election outcomes. There are still institutional, as well as statutory, barriers. Some general registrars do not necessarily understand how RLAs work and, understandably, confuse them with the existing law, which conflates machine audits with true RLAs. Registrars are taking a wait-and-see approach.[59]

Current LWVUS and LWV-VA Positions

LWVUS: Supports voting systems that are secure, accurate, recountable, accessible, and transparent.[60] LWVUS supports only voting systems that are designed so that…the paper ballot/record is used for audits and recounts; [and] routine audits of the paper ballot/record in randomly selected precincts can be conducted in every election, and the results published by the jurisdiction.[61]

LWV-VA: Positions do not address audits.

Study Committee Recommendation

The study committee recommends that the LWV-VA Election Laws position be modified to support post-election audits including

- Supporting a statutory requirement that risk-limiting audits be conducted in the Commonwealth after each election, which audits must be conducted in a transparent manner before the election is certified and with the potential to affect the outcome of the election.
- Supporting that ELECT conduct audits across jurisdictions if contests involve more than one jurisdiction

Part B: Prepare Amendment to State Position to Strengthen Support for Security, Including Physical Security of Voting Equipment and Ballots

B1. Security of Registration and Election Software Applications and Databases Throughout the Commonwealth of Virginia

Background

In 2017, Secretary of Homeland Security Jeh Johnson noted that "cyberattacks on this country are becoming more sophisticated…and dangerous." He designated election systems as a subsector of the existing Government Facilities Critical Infrastructure Sector, which enables the Department of Homeland Security (DHS) to prioritize cybersecurity assistance to those state and local election officials who request it. It also allowed DHS to monitor suspicious activity related to state election systems, and to issue alerts regarding attempted intrusions.[62] Intelligence officials believe that election systems in all 50 states have been probed.[63] Compromise of voter registration data through malicious modification, additions, deletions, or through ransomware or denial-of-service attacks would result in disruption at polling places on Election Day, disenfranchisement of eligible voters and/or casting of illegal votes, delay and expense in processing provisional votes, and loss of confidence in the outcome of an election.[64]

Federal agencies, including DHS's Cybersecurity and Infrastructure Security Agency (CISA)[65] and NIST[66], have developed cybersecurity best practices for critical computer infrastructure, including actions to combat risks specific to voter registration databases.[67] The Center for Internet Security (CIS) *Handbook for Elections Infrastructure Security* describes 54 best practices for network-connected election systems.[68] Daily innovation in techniques by cyberattackers makes it impossible to provide a comprehensive, static list of cyber defense strategies. To stay abreast of security alerts, CIS hosts the Multi-State Information Sharing and Analysis Center (MS-ISAC), which monitors networks and provides early warnings on cybersecurity threats.[69]

States are more likely than municipalities to have resources to engage highly qualified staff and to contract with cybersecurity experts to harden their systems. Ensuring that localities employ strong cybersecurity standards for access to the central system is constrained by the independence of each jurisdiction. Cost, resources, and resistance to central authority may hamper a state's ability to fully secure interfaces to the election system.

Virginia's Voter Registration Database

The Virginia Election and Registration Information System (VERIS) was implemented in 2007.[70] In 2019, a Joint Legislative Audit and Review Commission assessment found that VERIS was not sufficiently functional or reliable.[71] ELECT plans to implement a new system in 2022 if the General Assembly provides funding.[72]

VERIS runs on infrastructure managed by the Virginia Information Technologies Agency (VITA), which has adopted standards of NIST for computer security.[73] VERIS provides interfaces for three types of users:

- ELECT staff, who access VERIS using VITA-managed computers over the Commonwealth Virtual Private Network (VPN)
- General Registrars, who access VERIS from locality computers using two-factor authentication
- Citizens, who access the online registration portal over the internet from the Department of Motor Vehicles (DMV) or from an independent computer

New voter registrations are entered from paper forms or submitted electronically, and they must be approved by the General Registrar in a voter's locality. Changes or deletions to the voter list are based on data that ELECT receives from the Department of Motor Vehicles, the National Change of Address database, the Bureau of Vital Statistics, the multi-state Election Registration Information Center, and

court records.[74] General Registrars are responsible for assigning voters to precincts based on their addresses. These data are used to produce extracts of the registration list to be loaded onto EPBs, or to create printed pollbooks for localities that do not use EPBs.[75] At the close of an election, General Registrars are responsible for entering vote counts into VERIS for each contest in their locality. They also upload or manually enter "voter credit" data to indicate which voters participated in the election. VERIS tabulates the vote counts and exports data to the Election Reporting System for communication of the results.[76]

Virginia has 133 localities that vary widely in population and resources. The knowledge and financial capabilities required to safeguard computers used for VERIS access are scarce in some localities. If local systems are also used to run other office or personal applications, a staff member may unintentionally compromise the integrity of the connection to VERIS. For example, internet browsing or accessing email on an insufficiently protected computer could introduce malware that attempts to breach the central computer's defenses.[77] The use of removable storage devices, such as USB drives, to download pollbook data or upload voter credit data introduces another means of introducing malware to the system.[78] Providing a web portal for voters to view and maintain their own information makes voter registration more accessible to citizens. However, it also offers a possible avenue for cyberattack.[79]

In 2019, Virginia enacted legislation requiring the development of standards to ensure the security and integrity of the voter registration system and the supporting technologies used by localities to maintain that information.[80] ELECT is working with CISA to identify vulnerabilities and perform risk assessments; it requires localities to conduct annual cybersecurity self-assessments and to participate in one of CISA's information sharing and analysis centers.[81] In its narrative budget regarding use of 2018 HAVA funds, ELECT proposed "to substantially increase the security posture of the election infrastructure used in the Commonwealth of Virginia through cost-effective implementation of the standards, policies and best practices" developed by VITA and federal standards-issuing agencies.[82]

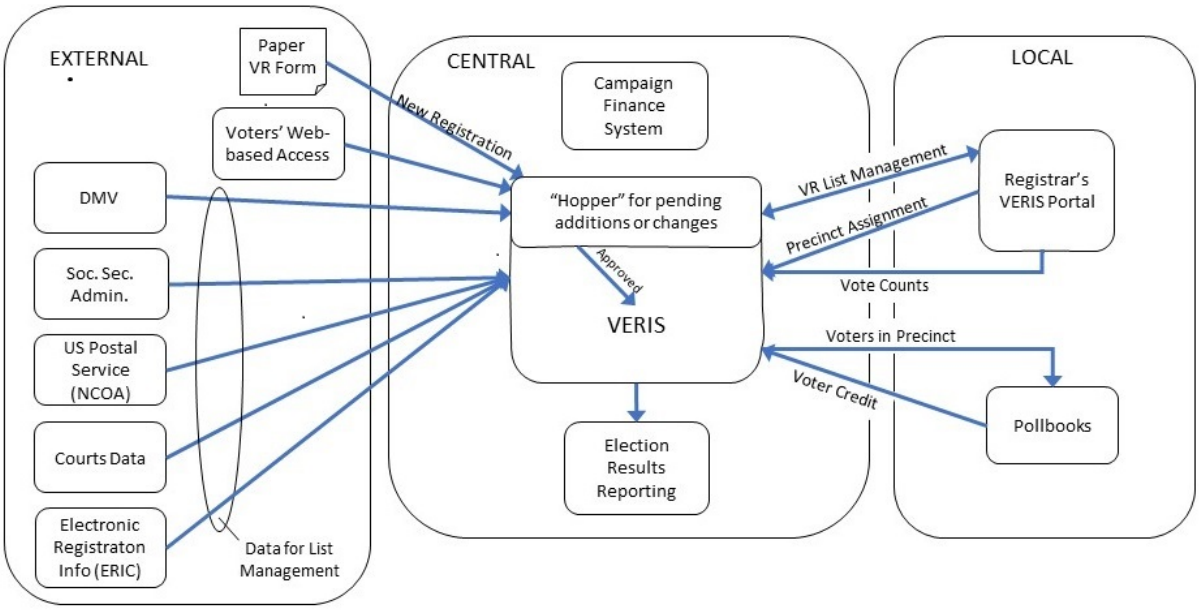

Figure 1: A simple representation of VERIS and its interfaces[83]

ELECT has a culture that supports strong cybersecurity practices and is moving toward increasing its defensive capabilities. The state currently participates in MS-ISAC and is working with consultants to bring best-practice cybersecurity to its central election system. The Governor's 2020 budget proposal would fund new staff in ELECT's IT and Training areas.[84] Recent legislation requires

ELECT to work with localities to ensure that vulnerabilities in remote access are addressed. ELECT has plans to upgrade or replace VERIS in the near future. This progress should be supported and reinforced by the League's positions on election laws.

Current LWVUS and LWV-VA Positions

LWVUS: Supports voting systems that are secure, accurate, recountable, accessible, and transparent.[85] Five focus areas were identified by the League as essential to protecting the votes of all citizens and improving election administration overall, one of which is to improve administration of statewide database systems.[86]

LWV-VA: Positions do not address security.

Study Committee Recommendation

The study committee recommends that the LWV-VA Election Laws position be modified to address the security of registration and election software applications and databases including

- Ensuring that the Commonwealth provides sufficient resources for
  - adequately staffing central information technology functions and maintaining infrastructure and applications to a high level of cyberprotection
  - supporting localities in securing systems that access central registration and election applications
- Recommending that the Commonwealth participate in national and multistate associations that develop cybersecurity standards, monitor emerging threats to critical infrastructure, and identify protection strategies
- Supporting the acquisition and maintenance of a voter registration and election management system that meets high standards for security, usability, reliability, and functionality

B2: Cybersecurity of Election Equipment, Including Electronic Pollbooks, Local Election Management Systems, Ballot Marking Devices, and Optical Ballot Scanners.

Background

Election Management Systems (EMS)

An EMS is an integrated suite of applications that can be used in local jurisdictions for "back office" tasks related to elections. The primary tasks are to define the content of a ballot, create a ballot layout, create files that control the operation of ballot marking and tabulating devices, and accumulate the voting results from multiple precincts to produce a local tabulation. The EMS generally resides on an off the shelf (COTS) computer in a locality's central office and sends data to and receives data from precinct-level devices via removable media such as USB drives.[87] Using the EMS computer for email raises the risk of a successful "spear-phishing" attack on the system.

If malware is introduced into the computer on which the EMS runs, then infection of ballot definition file media can occur.[88] This is more likely if the computer is also used for web browsing, music streaming, email, etc. Removable media are vulnerable to cyberattack if they are used for any purpose other than transmitting ballot definition files, can be accessed by unauthorized persons, or are from sources whose security practices cannot be verified.

Because of the technical complexity of the task, some localities delegate the creation of ballot definition files to the voting system vendor's personnel or other consultant. Vendors and contractors may have access to sensitive data such as ballot layouts, device configurations, and voter data that could be exposed if stored outside the jurisdiction's control.[89]

Ballot Marking Devices (BMD)

BMDs provide an interface (e.g., tactile keyboards, ports for headphone jacks or sip-and-puff devices) to assist voters who have accessibility needs that interfere with marking a paper ballot; BMDs produce a marked ballot which is then scanned or counted manually. The BMD prints a ballot that is either identical to ballots marked by hand or is a summary of the voter's choices.[90] The advantages of BMDs (other than their assistive features) are that they create unambiguous selection marks, prevent overvoting, and warn about under-voting. The disadvantages are that they are complicated to manage and operate, and that they put the onus onto voters for discovering and reporting discrepancies on a machine-marked ballot.[91]

BMDs are special-purpose computers that are vulnerable to error as a result of hacked or corrupted ballot definition files or infected removable media. The ports that allow insertion of a voter's assistive device also offer points of access for cyberattack. Of particular concern is that newer BMDs encode the voter's selections in a barcode for ease in scanning, as well as listing them in plain text. However, since the voter is unable to decipher a barcode, these devices could alter a voter's selections without the voter's awareness.[92] The National Election Defense Coalition opposes adopting ballot marking devices as the primary method of voting because they introduce unnecessary security risks, incur unnecessary expense, and are more likely to cause voters to wait to be able to vote.[93]

Optical Ballot Scanners

Optical mark recognition automates the counting of ballots and can generate a digital cast ballot image that can be used for auditing, or to simplify the interpretation of write-in votes, ballots that are empty, or ballots that have ambiguous markings.[94] When the ballot is scanned, the devices detect marks in specific areas. The scanners are required to identify overvotes and to enable voters to retrieve and discard their ballots before receiving replacement ballots. Ballot scanners can also warn voters, before the ballot is counted, if undervotes or ambiguous marks are detected. Ballots on which write-in votes are sensed can be diverted to a separate section of the ballot storage box. At the close of polling, the device is opened to retrieve its vote tallies.[95] Scanners at the precinct level provide voters with the option of fixing an error. Central-count scanners are often higher-speed devices; they are generally used for counting absentee or mail-in ballots[96].

The advantage of tabulation by scanner is the speed with which votes can be processed, and the ability of precinct-based scanners to produce a count before the paper ballots are transported to a central location. Disadvantages include the limitations of a computer system to interpret human variation in making marks, potential malfunction of the devices due to environmental conditions or mechanical issues, and the inherent vulnerability of any computer system to attack. Fraudulent vote counting by an optical scanner is possible if a malicious actor were to gain access to configuration files or to the removable media used to transport those files to the scanners.[97]

Electronic Poll Books

There are no national standards for the security and operation of electronic pollbooks.[98] The utility of electronic pollbooks depends on their ability to share up-to-date information across devices and locations, which poses inherent cybersecurity challenges. Lists of registered voters and other related information (e.g., whether a voter has cast an absentee ballot) must be transferred onto electronic pollbooks. After an election, information must be exported from the pollbook and transferred back to the local and state election offices. Any transmission of information represents a security risk. CIS states that breaching of or tampering with voter information is more likely to occur within voter registration systems "but could also occur in the e-pollbooks themselves and during the transmission of data to the e-pollbook."[99]

In 2018, NAS proposed three recommendations for electronic pollbook security.[100] First, jurisdictions should establish backup plans in case of electronic pollbook malfunction. Second, Congress should authorize and fund NIST to develop security standards and protocols for electronic pollbooks.

Finally, NAS recommends that election administrators develop security plans and procedures for assessing and testing electronic pollbook vulnerabilities. The Brennan Center also recommends:

- Limit or eliminate connectivity to wireless networks (including Bluetooth) whenever possible.
- Implement proper security protocols when wireless connectivity is required (e.g., when using devices like iPads that do not support a wired connection).
- Ensure that systems are properly patched as part of Election Day preparations.
- Keep appropriate backup of voter registration information in polling places.
- Provide sufficient provisional ballots and materials for two to three hours of peak voting, in case of electronic pollbook failure.
- Train poll workers to implement pollbook contingencies. [101]

Best Practices for Electronic Voting Systems

CIS's *Handbook for Elections Infrastructure Security* presents 17 best practices for election system components that are "indirectly connected", i.e., without persistent network or wireless connectivity but utilizing removable media for transfer of data between devices.[102] Their high priority recommendations cover the following topics:

- Separate the election management system from all activities and applications that are not election-related.
- Limit physical access; restrict the number of staff who can access the system or device; employ strong access controls; remove default credentials.
- Ensure all devices have the latest security patches and software updates; implement a change freeze prior to major elections.
- Store master images of application and device software on a securely managed offline system; verify the validity of the code base through hashing algorithms or other accepted procedure.
- Disable wireless capability; prohibit remote access.
- Configure systems to recognize only specific removable media devices (i.e. by serial number); encrypt data transferred by removable media; use write-once media for transferring critical files; control physical access to all removable media.
- Utilize tamper evident seals on all external ports that are not required for use.
- Document an Acceptable Use policy that details appropriate use of the system and all election-related data.
- Ensure staff is trained in cybersecurity and audit procedures.
- Conduct criminal background checks for all staff including vendors, consultants and contractors supporting the election process; conduct regular independent audits of their security controls.
- Perform system testing on all devices prior to elections; conduct acceptance testing when installing new or updated software or new devices.

Other cybersecurity and election experts have published recommendations that reinforce and extend this list of best practices. NAS calls for states and local jurisdictions to have policies in place for routine replacement of election systems, to avoid the security risks of obsolete systems[103]. The Belfer Center at Harvard's Kennedy School notes that best practices for prevention of cyberattack must be accompanied by procedures for detection (such as testing, monitoring and auditing) and recovery (such as offline backups and alternate manual procedures), and highlights the need for oversight of vendors and contractors. Requests for proposals, acquisition, and maintenance contracts should include explicit security stipulations to ensure that vendors follow appropriate security standards[104]. In a letter to Congress, the National Election Defense Coalition focused on three high-level objectives for ensuring election integrity:

1. Establish voter-verified paper ballots as the official record of voter intent.

2. Safeguard against internet-related security vulnerabilities and assure the ability to detect attacks.
3. Require robust statistical post-election audits before certification of final results in federal elections.[105]

Election Equipment in Virginia

Virginia's 133 localities are responsible for purchasing, managing, and operating devices that support the election process. Each Board of Elections may choose among the systems that have been certified by Virginia. In 2019, four vendors supplied voting devices in Virginia. The devices included five models of ballot marking devices (BMD), ten models of optical scanner, and one hybrid BMD/scanner model.[106]

Each locality is required to provide vote casting methods that accommodate different physical abilities and, depending on local demographics, different languages.[107] This generally means that at least one ballot-marking device with special adaptations is available in a precinct, even if most voters vote by hand-marking a paper ballot. Ballots may be counted by optical scanners or by direct recording electronic (DRE) devices that produce a record of each vote. Thus, each locality has a particular suite of devices that must be properly configured and maintained. In 2016, the Code of Virginia was amended to prohibit DREs after July 1, 2020.[108]

Virginia law[109] requires voting systems to pass state certification standards, which in turn mandate that the systems have first achieved certification by the Election Assurance Commission (EAC). The standards are intended to establish baseline functionality, accessibility, and security of systems.[110]

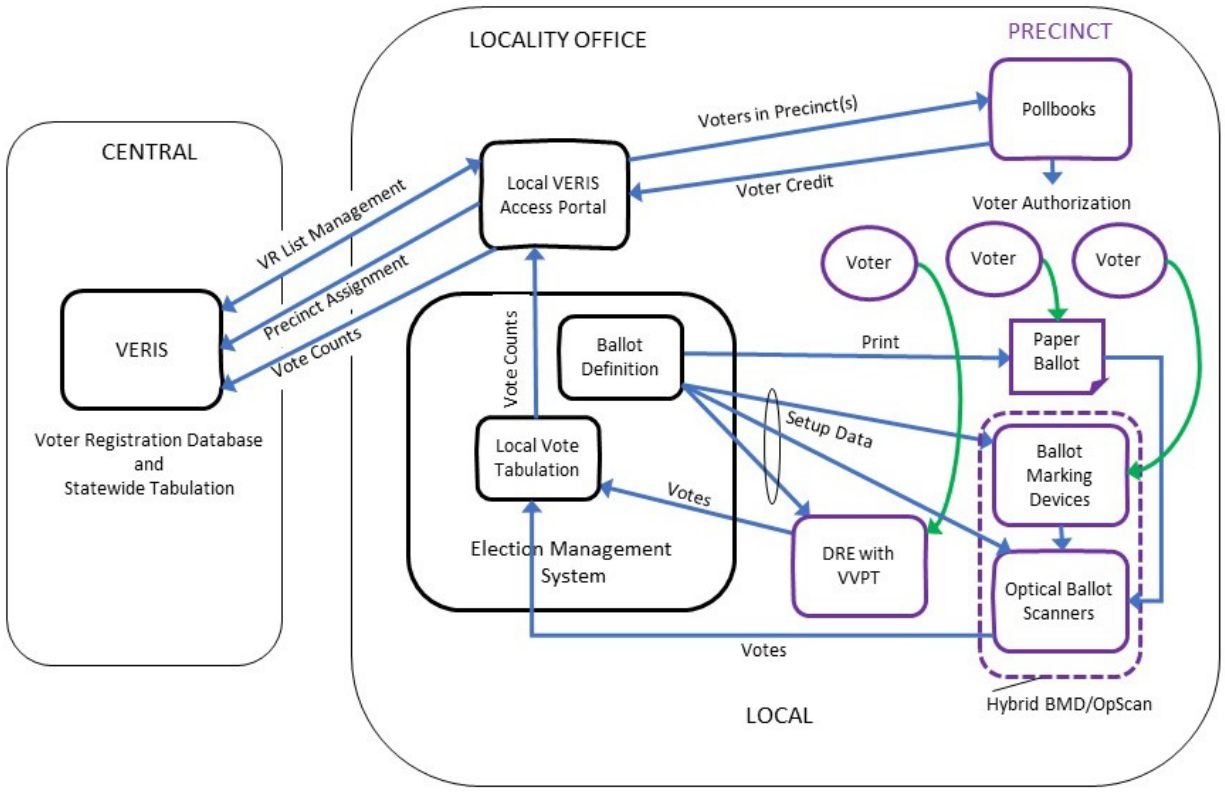

Figure 2: A simplified diagram of the possible components of a locality's election infrastructure[111]

As shown in Figure 2, electronic voting systems are comprised of interrelated components: a local election management system, ballot marking devices, optical scanners, and (until July 2020) DREs.

These components are considered one unit for the purpose of federal and state certification. Although each device has unique vulnerabilities, they also share certain risks and benefit from similar cybersecurity best practices.

Before a local electoral board can place a voting system into operation, it must pass acceptance testing.[112] Voting systems also undergo logic and accuracy (L&A) testing for every ballot style and system component both prior to and immediately after the election. The EAC recommends producing and processing a set of pre-audited votes and comparing the counts to the expected results.[113] The test must be observed, and the results certified by an electoral board member, general registrar, or a designated representative. Vendor personnel must not conduct either acceptance or L&A testing.[114]

The number of assistive interfaces in a BMD makes it nearly impossible to conduct a manual test of every device, ballot style, and language. Although Virginia requires that localities conduct L&A testing, no standards have been developed to assist local election officials to perform these tests adequately.

Virginia law allows for both paper and electronic pollbooks; jurisdictions may use their own funding to purchase electronic pollbooks, as long as they are approved by the state.[115] Electronic pollbook systems used in Virginia are designed by third-party vendors; they use off-the-shelf hardware (e.g., iPads) and proprietary software.[116] Whether due to malicious attacks or just malfunctioning equipment, issues with electronic pollbooks can cause long wait times and affect voter confidence. Virginia law does not require jurisdictions to keep paper backups at polling places when electronic pollbooks are in use, though some jurisdictions do.[117] If technical issues prevent use of the electronic pollbooks and there is no backup available, all affected voters must vote a provisional ballot.[118]

The SBE has developed procedures and system requirements for electronic pollbooks. Localities perform acceptance testing when they receive new electronic pollbooks; however, the state leaves pre-election testing to the discretion of the locality.[119] Unlike other election equipment, electronic pollbooks are often networked to allow information to be sent from one pollbook to another so that, for example, all the pollbooks in a given precinct indicate whether a particular voter has checked in. Virginia's certification standards have specific requirements for connection, encryption, and authentication to protect the integrity of networked electronic pollbooks, and pollbooks may never be connected to a publicly accessible network.[120]

The 2019 update to the Code of Virginia § 24.2-410.2 [B][121] mandates that localities annually submit written plans and procedures for the security and integrity of technologies used to access the central voter registration database. In November 2019, the SBE approved a package of twenty minimum security standards presented by the ELECT. The motion to approve these standards stated that "In support of improving elections security maturity within the Commonwealth prior to the 2020 Election, localities are highly encouraged to align their resources to assure that at a minimum, the standards identified with a Risk Priority of critical and high, are implemented by September 1, 2020 – along with any others they believe to be of critical and high risk priority for their locality." ELECT worked with a selection of nine localities to develop cost estimates for implementing the standards. Within that diverse group, ELECT found that "Size of locality does not necessarily imply greater elections security maturity." and "Elections security maturity, even to these minimum standards, varies greatly."[122]

Current LWVUS and LWV-VA Positions

LWVUS: Supports voting systems that are secure, accurate, recountable, accessible, and transparent.[123]

LWV-VA: Positions do not address security.

Study Committee Recommendation

The study committee recommends that the LWV-VA Election Laws position be modified to address the cybersecurity of election equipment including

- Supporting the use of BMDs that produce ballots identical to hand-marked ballots to avoid vulnerabilities associated with barcodes
- Supporting the use of standards for logic and accuracy testing of election equipment
- Requiring standards for security practices of voting machine vendors, their personnel and consultants/contractors
- Supporting the replacement of devices well before end of life.
- Recommending that the Commonwealth and localities have sufficient resources to follow best practices for cybersecurity
- Requiring the use of paper backups of voter lists (or other contingency plans) in case of electronic pollbook malfunction

B3. Physical Security

Background

Physical election security should take a broad view, focusing not just on the election machines but the entire voting system including buildings, personnel, documentation, and operating procedures. The first step towards assuring physical security is knowing what equipment is owned, controlling how it is stored and maintained, and documenting changes to system components, both hard and soft. Documentation must be kept current, and obsolete information purged. The EAC recommends detailed inventory and ID tags, and keeping a log of all changes to the system, whether a simple inspection, or a change to a part, etc.[124]

Voting machines and paper ballots need to be kept securely stored. Access to equipment should be documented and limited to as few individuals as possible, with additional access only as needed, such as for repair/maintenance. EAC guidelines state that any unauthorized physical access, either to machines or paper ballots/ballot boxes, will leave evidence of that access.[125] A 2009 LWVUS study noted that physical protection of voting systems includes pre-election preparation and how components are secured during delivery to polling places, including locations for in person absentee voting.[126]

Ensuring physical security goes beyond protecting against malicious attacks. Proper security procedures include making sure voters and poll workers cannot inadvertently disrupt the election by, for example, accidentally turning off or disabling a machine. Polling places should be set up to so allow poll workers to easily monitor the voting equipment/procedures and identify any disruptions.[127] The Brennan Center also identifies emergency procedures and contingency plans as important components of security and recommends that poll worker instructions and training should anticipate likely scenarios and documentation procedures should be able to account for non-standard situations. [128]

The voting process requires integrity at every step of the supply chain. The Brennan Center reported that three vendors account for more than 80% of voting systems in use today.[129] This includes not just the voting machines, but electronic poll books, voter registration databases, ballot design, and configuration of voting machines. In contrast to vendors in other critical infrastructure sectors, these vendors receive little or no federal oversight. The Brennan Center has proposed a framework for oversight that includes issuing vendor best practices in the areas such as personnel and supply chain integrity, and expanding EAC's existing voluntary certification program to include vendors. This takes a step back in the election process and asks to know more about the vendors and their subcontractors, such as personnel policies for vetting employees, where parts come from, and how they are kept secure.

EAC's draft VVSG 2.0 principles describe voting system designs that are physically robust, easy for voters to use, and straightforward for evaluators. Several of the VVSG 2.0 principles will be relevant to the physical integrity of voting systems. Principle 12 focuses specifically on physical security and requires that

"12.1-The voting system prevents or detects attempts to tamper with voting system hardware.

12.2-The voting system only exposes physical ports and access points that are essential to voting operations."[130]

Physical Security in Virginia

ELECT publishes a handbook of procedures and guidelines for local elections officials, and many physical security items are codified in Virginia statutes. Local electoral boards are responsible for the security of their voting system, including electronic poll books. Additionally, localities are required to have a written security plan that is reviewed annually.

Law related to election security in Virginia is changing as a result of HB 2178, which passed during the 2019 legislative session. The bill is summarized on the Virginia Legislative Information System[131] as follows:

> **Virginia voter registration system; security plans and procedures; remedying security risks.** Directs the State Board of Elections to promulgate regulations and standards necessary to ensure the security and integrity of the Virginia voter registration system and the supporting technologies utilized by the counties and cities to maintain and record registrant information. The local electoral boards are also required to develop and update annually written plans and procedures to ensure the security and integrity of the supporting technologies. The local electoral boards are further required to report annually to the Department of Elections on their security plans and procedures. The bill authorizes the Department of Elections to limit a locality's access to the Virginia voter registration system if it is determined that the county or city has failed to develop security plans and procedures or to comply with the security standards established by the State Board; such access would be limited as necessary to address and resolve any security risks or to enforce compliance...The bill requires the State Board of Elections to convene a work group prior to adopting security standards and to establish a standing advisory group of local government IT professionals and general registrars to assist and consult on updates to security standards.

Voting Machines

As of 2018, Virginia requires testing to federal standards.[132] The basic requirements for protecting voting machines and election processes are laid down in the Code of Virginia Title 24.2 Elections.[133] Governing all aspects of security is the confidentiality about procedures that must be maintained at the Electoral Board level and downward.[134]

Counties may acquire different types of voting equipment that they deem appropriate to their locations, provided the equipment has been approved by the state. The Virginia Code says that jurisdictions shall employ dedicated staff, called custodians, to prepare and test the machines before an election. They are sworn officers who, in the presence of a member of the Electoral Board or the registrar and a member of political parties and/or a member of the public, put the machines through their paces and then seal them, numbering the seals as prescribed in the Code. Some localities, however, opt to contract the L&A testing to vendors' technicians, often because they lack sufficient IT staff capabilities to perform those testing functions in-house.

There is no explicit mention in the statute of storing all equipment in locked warehouses or lockable polling place location just before elections, but that is a precaution followed by election office personnel.

Election officers must be trained in the use of the equipment, which must be placed so that all machines are in full view. The officers who receive pollbook cartridges, keys, and seals in sealed envelopes at the beginning of the day must certify that these envelopes have been received. At the end of the day the items must be placed in sealed envelopes and signed. Representatives of the two major parties or candidates themselves must witness the sealing and signing.

After the officers of election have fully accounted for and stored the ballots and any aberrations and have signed the statement of results, one of the officers must take the ballots, pollbooks, and all materials in sealed envelopes to the clerk of the court, who retains custody of them, keeping the sealed boxes in a secure place, waiting until the period for a recount request has passed.

An informal survey of LWV-VA members who serve as election officers, showed that the respondents had a high degree of confidence in the security procedures observed in their polling places. One of the respondents is a registrar. The survey is Appendix B.

Electronic Poll Books

Poll book records, paper or electronic, are transmitted to the SBE on USBs in sealed packages for voter credit just after an election, then returned to the registrar to be kept for two years. Election officers in the polling places certify the names and numbers of qualified voters who have voted. The EPB is marked to identify the election for which it is used.

Voter Registration Machines

The main vulnerability of VERIS is in the cybersecurity realm, but there are physical protections. ELECT's Commissioner Piper explained that there are two locations for the database, one at the Commonwealth Enterprise Service Center in Chesterfield County and one at another location in Virginia managed by VITA. There are periodic reviews of permissions for access based on roles.[135] Under HB 2178, ELECT may limit a locality's access to VERIS if its security plans do not comply with state standards.

Looking Ahead

Under HAVA, Virginia received funding in 2018 of $9,080,731 to be spent over a five-year period for upgrading all aspects of the election system and personnel training. Commissioner Piper specified the deliverables in a letter to the EAC:

1. The Department of Elections will continue to provide multifactor authentication for all users accessing sensitive data.
2. The Department will provide effective cybersecurity training.
3. The Department will develop the new and updated standards and templates.
4. The Department will conduct training and provide guidance on the implementation of the standards.
5. Each voting system and electronic pollbook system will be recertified within 4 years, in accordance with the new certification standards.
6. The Department will establish a 4-year cycle for the review of all equipment certification standards.
7. The budget attached to this document shows a supplement of 5 percent approved by Governor Ralph Northam. [136]

In September 2019 Congress allocated another $250 million to give to states for election security but did not set any criteria for how it should be disbursed or spent. Funding depends on the will of Congress to release it; there is no regular schedule or pattern.[137]

It must be emphasized that the development of security procedures of all kinds in Virginia is very dynamic right now. ELECT announced that it has approved the new minimum security standards developed after the passage of HB 2178 to take effect during 2020.[138] The new standards are mainly focused on cybersecurity, but there are improvements in statewide standardization, such as new certification requirements for electronic pollbooks to enable them to function well during no excuse absentee voting.[139] There are many provisions for staff training on such matters as incident response and contingency planning. Election administrators must submit annual reports and are responsible for risk assessment. The local Electoral Board is accountable for its locality.

Physical access to equipment by personnel, vendors, and maintenance staff is limited and documented. There should be no superfluous connecting materials. Maintenance tools are permitted only to authorized personnel. Any equipment that may be taken out of the facility cannot have a label indicating its locality. Badges and keys are secured. To prevent incidents, there are recommendations for the maintenance of the environment, such as temperature and humidity control, cable repair, and an uninterruptible power supply.[140]

Current LWVUS and LWV-VA Positions

LWVUS: Supports voting systems that are secure, accurate, recountable, accessible, and transparent.[141]

LWV-VA: Positions do not address security.

Study Committee Recommendation

The study committee recommends that the LWV-VA Election Laws position be modified to address physical security including

- Supporting the use of recountable, voter-verifiable paper ballots marked either by hand and scanned or by a ballot-marking device that produces a paper or card ballot
- Developing minimum standards to protect the equipment used in all phases of the voting process, from computers that hold the database of registered voters to electronic poll books and electronic voting machines.
- Requiring appropriate and systematic training of permanent personnel and polling place election officers

Part C: Review Language Supporting Electronic Voting

Background

In the context of this study, "electronic voting" is more accurately described as "internet voting" or "online voting," because the reference is to voting via the internet. Online or internet voting includes not only voting directly from a device such as a computer, tablet, or smartphone but also the attachment of an absentee ballot to an email, and sending by facsimile (fax).[142] Making voting accessible to voters who face obstacles to voting in person or absentee by mail is a compelling goal. Citizens with disabilities and voters overseas, notably our military, should be able to vote with the same convenience as those at home. The issue is whether the convenience outweighs the risks that internet voting poses to election systems and outcomes.

Internet voting has been subject to study and pilot projects for years, internationally as well as in the United States.[143] In the U.S., West Virginia, Utah, and Denver have piloted internet voting through mobile phone applications. Arizona, Colorado, Missouri, and North Dakota allow some voters to return ballots using web-based portals. Nineteen states and Washington, DC allow some voters to return ballots via email or fax.[144] In 2018, West Virginia became the first state to test internet voting through a mobile application in federal elections by initiating a pilot available to overseas voters in certain counties. In the pilot, 183 people requested the mobile application, 160 downloaded it, and 144 (78.7%) cast votes.[145] A 2019 survey found that West Virginia voters living abroad who could vote online were 3-5% more likely to vote than those who did not have access to this technology.[146] Denver piloted mobile voting for military personnel and citizens stationed overseas in the 2019 municipal general election. This pilot also had a high completion rate—120 out of 156 (76.9%) ballots were returned—although the self-selection of voters participating in the pilot could explain the high rate of return.[147]

Arguments in Favor of Internet Voting

Internet voting has three primary advantages: (1) it is generally more convenient, and increased convenience may increase voter participation; (2) it enables specific populations, such as overseas voters and voters with certain disabilities, to vote more easily; and (3) it may improve accuracy and efficiency of vote counting.

Internet voting is convenient since the voter does not have to travel to a polling place or wait in line to vote. Initiating online voting takes some time—each voter has to download and learn to use a mobile application, verify his/her identity, and then vote—yet, this is likely less time consuming than voting at a polling location. Internet voting is also more efficient than voting by mail; to vote by mail, a voter has to request a ballot, wait for it to arrive, fill it out, find postage, and mail it back. Voters who request ballots online need to be able to print the ballots.

In 2016, it was estimated that 5.5 million US citizens lived overseas.[148] The Military and Overseas Voter Empowerment (MOVE) Act requires that ballots be sent to these voters no less than 45 days before Election Day. Despite this, only 26% of active duty military members cast ballots in 2016 and 21% of ballots mailed to citizens were returned to local election offices as undeliverable.[149] Overseas military voters face obstacles in transmitting and receiving election-related materials including slow mail delivery and lack of secure mailing systems.[150] A Federal Voting Assistance Program analysis found that voters who retrieved their ballots online were nearly 50% more likely to vote successfully.[151]

For voters with disabilities, casting ballots on mobile phones could be significantly easier than travelling to the polls.[152] While the Americans with Disabilities Act requires that people with disabilities have access to public services such as voting, barriers remain, both in terms of a shortage of voting machines with accessible features and physical barriers. In 2016, the Government Accountability Office examined the outside areas of 178 polling places and found that 60% had potential impediments.[153] Mobile phones have features that can help voters with a range of disabilities; phones can increase text size, read the screen's content aloud, and operate through voice commands.

Internet voting systems record and store ballot selections more efficiently than traditional voting systems. It is much faster to tally mobile votes than tallying votes from paper mail-in ballots. The software can prevent voter error when filling out a ballot and decrease chances of ballot invalidation. For example, the software can be programmed so that it only allows the voter to choose the right number of candidates for each office. Importantly, election officials are more easily able to monitor relatively small voting populations using an internet voting application for potential compromises.[154]

Arguments Opposed to Internet Voting

Election security experts emphasize that elections must be anonymous, secure, accessible, recountable, and verifiable. Numerous vulnerabilities are created by online voting, including:

- The inability to accurately authenticate the voter's identity (forged credentials, limitations of facial recognition software and lack of biometric data)
- System disruption, such as denial-of-service attacks that slow or crash a system
- Malware on voters' devices that can modify votes undetectably
- Attacks on servers and routers from remote locations through malware-infested transmissions
- Manipulation by either outsiders or insiders (equipment manufacturers, technicians, and others with legitimate access to election software or data) to undetectably change votes
- Spoofing, which would direct voters to a phony elections website instead of the real one
- Voter coercion, such as the use of cryptocurrency to buy and sell votes[155,156,157,158]

A computer scientist who studies online voting explains, "[O]nline elections might be compromised and the wrong people elected via silent, remote, automated vote manipulation that leaves no audit trail and no evidence for election officials…to even detect the problem…."[159]

Some states have backed away from internet voting. Alaska, which stood to benefit from internet voting because the population is so spread out and isolated, discontinued its web portal for online ballot

transmission, and Washington state rescinded permission for all but a few voters to return ballots over the internet in 2018; in both states the vulnerabilities became manifest to their authorities when they visited a hacker convention.[160]

Some proponents argue that technologies such as blockchain, a technology intended to keep information secure, are the answer. Critics contend that "[Blockchain] fails to address many of the fundamental and universal security challenges inherent to online voting…"[161] Blockchain technologies do not permit voters to verify the actual ballots tabulated and ballots cannot be audited. NAS notes that blockchain fails to preserve voter anonymity and ballot secrecy and "do[es] not redress the security issues associated with Internet voting."[162]

Another system, end-to-end (E2E) verifiability, can provide online voting that allows voters to ascertain that their votes were recorded correctly and that their votes were included in the final tally, and is generally auditable.[163] But E2E systems are as prone to malware and denial-of-service attacks as any other system and do not address voter authentication.[164]

In 2019, Alex Halderman, a computer science professor known for commandeering an online voting system as a white-hat hacker,[165] held up his smartphone and wryly forecast that someday everyone will vote using a personal device.[166] Nevertheless, in Virginia, the current Commissioner of Elections recognizes that the technology is not "there" to permit online voting.[167] A 2018 NAS analysis noted that "Insecure Internet voting is possible now, but the risks currently associated with Internet voting are more significant than the benefits. Secure Internet voting will likely not be feasible in the near future."[168]

Status of Internet Voting in Virginia

Virginia has entertained legislation to study or to pilot internet voting in recent years.[169] Despite an in-depth study, which included a framework for internet voting, the method has never been tested in the Commonwealth.[170]

A 2015 report by ELECT pointed out some of these vulnerabilities and added others, such as phishing; ballot interception, which could either prevent a voter from receiving a ballot; and ballot spoofing, where a malicious actor either swaps out a real ballot or modifies it before it reaches the voter.[171] An author of the report points out that cyberthreats have become increasingly mature and ubiquitous, and that he would have greater reservations about internet voting today than he did when the report was prepared.[172]

The 2020 Virginia General Assembly approved an extension of the deadline for returning absentee ballots and extended the deadline for applying for absentee ballot by mail for all (not just MOVE) voters. [173]

Current LWVUS and LWV-VA Positions

LWVUS: Supports voting systems that are secure, accurate, recountable, accessible, and transparent.[174]

LWV-VA: Supports the use of electronic means for submitting absentee ballots by military and overseas voters if it can be accomplished while maintaining ballot security and integrity.[175]

Study Committee Recommendation

The study committee recommends that the current LWV-VA Election Laws position be modified to include

- Opposing the return of voted absentee ballots utilizing any aspect of the internet unless and until such voting can be accomplished while maintaining ballot security and integrity, the security of elections systems, voter anonymity, and ballot secrecy

Part D. Add a Statement Opposing the Requirement for Photo ID at the Polls

Background

Information in this section is based on the recollections and personal records of Therese Martin,[176] the LWV-VA Public Advocacy for Voter Protection Coordinator at the time, and Olga Hernandez,[177] former president of LWV-Fairfax Area.

Under the LWVUS position opposing photo IDs, LWV-VA argued against SB 1256, the bill requiring that citizens present a photo ID at the polls in order to be eligible to vote, which was passed in 2013 and became effective July 1, 2014. Many other civic organizations also opposed passage. Reasons for opposition included the high cost, the difficulty for some people in obtaining a photo ID, its restrictiveness, and the lack of evidence of fraud by voter impersonation. Though unsuccessful at preventing the photo ID requirement, these organizations did effect changes in the language of the bill—the final bill wording became, "the State Board shall provide free voter registration …" [emphasis added].[178]

Civic organizations did convince the General Assembly to liberalize the mandate to the SBE, requiring that it provide equipment for local registrars to obtain photos and signatures of voters who requested ID cards, without cost to the registrars.[179] An Executive Order was issued requiring the SBE to ensure that local jurisdictions had resources to educate the public effectively about the new law. ELECT developed a coordinated "Are You Election Ready?" campaign employing all forms of media, including social media, to inform citizens about the new requirement. Civic organizations worked with the election offices and one another to publicize the new requirement and the availability of the free photo ID.

However, the campaign depended on the ability of general registrars in each jurisdiction to implement the new requirements. Some provided their staff with photo equipment to take to libraries, community centers, and even senior residences. A survey of the 133 registrars found only 9 who definitely planned to take photo equipment into the field and 38 who might. Only one set of equipment was provided to each jurisdiction, regardless of its geographical area or size of population.

After the general election in November 2014, the League surveyed its members, many of whom served as election officers, about their observations concerning the photo ID law. The survey indicated very few problems, but members reported that the people who did not have current photo IDs were elderly persons who had recently moved. Further, the survey indicated that those voters either no longer drove and did not have another photo ID, or they had trouble getting new IDs because of issues with the documents they did have. Women who have changed their names are disproportionately affected.[180] The Brennan Center also reported anecdotal evidence that there were inconsistencies in the way the new law was implemented in some polling places. Some voters in Virginia who did not have photo IDs were not given provisional ballots.[181]

ELECT reports the number of persons voting provisionally, including those who did not have an appropriate ID, but does not say why voters had no ID. In 2014, 773 (21%) of those who voted provisionally had no appropriate ID. In 2019, 611 (~20%) voted provisionally because they had no ID, about the same as in 2014.[182] There is no data on the number of potentially eligible voters who did not go to the polls because they lacked photo ID.

The photo ID rule was reviewed and upheld by federal courts in 2016.[183] Several former state and local election officials testified at the trial that they were not aware that anyone was unable to vote because of the lack of photo ID. They said that some voters probably did not follow up their provisional votes by sending a valid photo ID to the registrar's office.[184] Ultimately, the US Court of Appeals for the Fourth Circuit upheld Virginia's photo ID law on the grounds that the state's law was flexible and did not exhibit an intent to discriminate.[185]

Current Status in Virginia

Bills eliminating the photo voter identification requirements were enacted in the 2020 General Assembly session: HB 19 (Delegate Joseph C. Lindsey)[186] and SB 65 (Senator Mamie E. Locke).[187]

Additionally, this legislation allows voters without any permissible ID to sign an affidavit attesting to their identity. Under the new rule that eliminates the requirement to show a photo ID, though such an ID will still be accepted, voters will still be required to show some other form of identification, such as a voter confirmation document, a copy of a current utility bill, a bank statement, a government check or paycheck or other government document that shows the name and address of the voter. These forms of identification were formerly accepted in Virginia..

Under HAVA of 2002, a person who wants to vote in a federal election but does not show one of the federal required forms of identification may still vote provisionally using Virginia required ID's or an affidavit.[188]

Current LWVUS and LWV-VA Positions

LWVUS: Five focus areas were identified by the League as essential to protecting the votes of all citizens and improving election administration overall, one of which is to oppose photo ID and documentary proof-of-citizenship.[189]

LWV-VA: Positions do not address photo ID.

Study Committee Recommendation

The study committee recommends that the LWV-VA Election Laws position be modified to include

- Opposing the requirement that a voter present a photo ID at his or her polling place in order to be able to vote

Appendix A
Excerpts of LWVUS and LWV-VA Positions on Election Law

Excerpts from LWVUS position in the Representative Government section of *Impact on Issues, 2018-2020,* are in plain text below. For the full position, please see:
https://www.lwv.org/sites/default/files/2019-04/LWV 2018-20 Impact on Issues.pdf

Excerpts from LWV-VA Election Laws position in *Positioned for Action, 2019* are in italics below. For the full position, please see:
https://lwv-va.org/wp-content/uploads/2019/06/lwv-va-positions-Full-2019-Final-6-2-19.pdf

LWVUS Principles may "serve as an authority for action" if the state does not have an explicit position on a particular topic. (LWVUS, p. 13; see also LWV-VA Bylaws Article 10, Section 1, p. 4)

Part A: Include election processes, laws, and regulations (e.g., post-election audits that ensure free and fair election results, transparency, security, and accountability).

- LWVUS supports the implementation of voting systems and procedures that are "secure, accurate, recountable, accessible, and transparent." (LWVUS, p.11)
- Leagues should also consult standards developed by the Election Assistance Commission (EAC) pertaining to voting systems when studying or improving their own voting systems. (LWVUS, p.16)

- *Position in Brief: The League of Women Voters of Virginia believes that democratic government depends on the informed and active participation of its citizens; that voting is a right and responsibility; and that election laws, regulations and administrative procedures should be uniformly designed and applied, and adequately funded to facilitate and increase voter participation throughout Virginia*. (LWV-VA, p. 2)
- *The LWV-VA supports: Legislation to allow all registered voters to vote absentee prior to Election Day without specifying a reason. Both choices–voting in person or by mail—should be offered. (This no-excuse absentee voting is sometimes called "early voting".)* (LWV-VA, p.4)
- *NB: Post-election audits are not specifically mentioned in the LWV-VA position*

Part B: Prepare amendments to the State position to strengthen support for security, including physical security of voting equipment and ballots and management of security during in-person absentee voting.

- LWVUS supports the implementation of voting systems and procedures that are "secure, accurate, recountable, accessible, and transparent" (LWVUS, p.11). At Convention 2006, [League] delegates further clarified this position with a resolution stating that the Citizens' Right to Vote be interpreted to affirm that LWVUS supports only voting systems that are designed so that:
    - they employ a voter-verifiable paper ballot or other paper record, said paper being the official record of the voter's intent;
    - the voter can verify, either by eye or with the aid of suitable devices for those who have impaired vision, that the paper ballot/record accurately reflects his or her intent;
    - such verification takes place while the voter is still in the process of voting;
    - the paper ballot/record is used for audits and recounts;
    - the vote totals can be verified by an independent hand count of the paper ballot/record;

- routine audits of the paper ballot/record in randomly selected precincts can be conducted in every election, and the results published by the jurisdiction. (LWVUS, p.16)

- *The LWV-VA document does not discuss verifiable paper ballots or audits. When that position was written, some precincts in Virginia were still using the Direct Recording Electronic (DRE) machines*

Part C: Review language supporting electronic voting using the Internet.

- Since 2013, LWVUS has promoted five key proactive election reform priorities:
  - secure online voter registration,
  - permanent and portable statewide voter registration,
  - expansion of early voting,
  - improvement of polling place management,
  - and electronic streamlining of election processes. (LWVUS, p.13)

- *Prior to the election the LWV-VA supports*
  - *The use of electronic means for submitting absentee ballots by military and overseas voters if it can be accomplished while maintaining ballot security and integrity;*
- *LWV-VA recommends these measures for ensuring and efficient voting process at the polls:*
  - *Electronic poll books, with back-up paper copies for emergencies*
  - *Appropriate precinct sizes and numbers of voting machines to minimize voting delays*
  - *Well-trained officers of election*
  - *Polling places selected to maximize voter participation and near public transportation where possible*
  - *Legislation to allow all registered voters to vote absentee without specifying a reason (LWV-VA, p.4)*

Part D: Add a statement opposing requirement for photo ID at polls.

- Five focus areas [are] identified by the League as essential to protecting the votes of all citizens and improving election administration overall:
  - Oppose photo ID and documentary proof-of-citizenship;
  - Improve administration of statewide database systems;
  - Guard against undue restrictions on voter registration;
  - Improve polling place management; and
  - Improve poll worker training. (LWVUS, p.11)

- *The LWVUS has national positions on issues such as opposition to requirements for photo identification and other measures that restrict access to registration and voting, and support of voting systems that are secure, accurate, recountable, accessible, and provide a voter verifiable paper trail. Therefore, those topics were not covered in the study and are not specifically addressed in the current positions (LWV-VA, p.3)*

Appendix B
Physical Protection of Voting Systems
Survey of Local Leagues

If you have served as an Election Officer, observed your Electoral Board, or observed members of the Registrar's Office preparing election machines before an election, please put a check or X in front of the measures that your jurisdiction's Office of Election takes.

Note that "Components of voting systems" include ballots, optical scanners, voting machines, electronic poll books, and precinct registers or physically vulnerable records.

Please return your survey to Sidney Johnson http://sidneyjohnson3@verizon.net by November 18, 2019.

Thank you very much for your help.

Certification and usability:

____Voting machines certified by the State Board of Elections

_____ for voters and poll workers before the election

_____Computers dedicated to producing a sensitive program are isolated from others, e.g. computers used for software for pollbooks are not used for anything else; only a few people use them.

Physical access and security measures:

Physical access restricted to all components of voting systems:

_____Prior to election
_____During delivery to poll worker's home or polling place
_____At the polling place
_____Canvass, a reconciliation of tapes from the machines with the Statements of Record
_____Audits
_____Inventory and documentation for all physical components, at all times before, during, and after the election

_____Recording of who has access to ballots and election-related systems and why that person has access

_____Secure storage of machines and ballots (both before and after use) delivered to poll worker's home or polling place, including locations for in-person absentee voting

_____Secure transmission of ballots to the location where they are counted, then stored.

_____Additional comments:_____

Your jurisdiction _____
This information will be used strictly to assess the coverage and scope of the survey results. No information identifying or reporting about specific jurisdictions will be released.

Source: Election Audits Task Force of the League of Women Voters of the United States. (January, 2009) Report on Election Auditing. League of Women Voters of the United States. p 7.

References

[1] League of Women Voters of the United States (LWVUS). (2019). *Proposed concurrence on electoral systems*. Retrieved from https://www.lwv.org/league-management/proposed-concurrence-electoral-systems

[2] League of Women Voters of the United States (LWVUS). (2018). Representative government. *Impact on Issues 2018-2020*, pp. 10-28. Retrieved from https://www.lwv.org/sites/default/files/2019-04/LWV 2018-20 Impact on Issues.pdf

[3] League of Women Voters of Virginia (LWV-VA). (2019, Spring). *Positioned for Action,* pp. 2-4. https://lwv-va.org/wp-content/uploads/2019/06/lwv-va-positions-Full-2019-Final-6-2-19.pdf

[4] U. S. Senate Select Committee on Intelligence. (2019, July). Russian active measures; Campaigns and interference in the 2016 election. *Volume 1: Russian efforts against election infrastructure with additional views*. Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

5 Valerio, M. (November 5, 2019). We now know that Russia specifically targeted Virginia elections in 2016. *WUSA9*. Retrieved from https://www.wusa9.com/article/news/local/virginia/virginia-elections-targeted-by-russia/65-0119894f-99e7-4abc-8aff-1aae97033a2d

[6] League of Women Voters of Virginia (LWV-VA). (2019, Spring). *Positioned for Action,* pp. 2. https://lwv-va.org/wp-content/uploads/2019/06/lwv-va-positions-Full-2019-Final-6-2-19.pdf

[7] United States Election Assistance Commission. *Voluntary Voting System Guidelines*. Retrieved from https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/

[8] United States Election Assistance Commission. *Voluntary Voting System Guidelines*. Retrieved from https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/

[9] Epstein, Jeremy. Association for Computing Machinery, U.S. Technology Policy Committee (December 2019). Personal communication.

[10] National Association of State Election Directors, public comment to EAC (3 May, 2019). *NASED Executive Board Comment on the Voluntary Voting System Guidelines*. Retrieved from https://www.nased.org/news/2019/5/3/comment-on-the-vvsg

[11] National Conference of State Legislatures (6 Aug 2018). *Voting System Standards, Testing and Certification.* Retrieved from http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx

[12] United States Election Assistance Commission. Technical Guidelines Development Committee (28 March 2019). *TGDC Recommended VVSG 2.0 Principles and Guidelines (Draft)*. Retrieved from https://www.eac.gov/assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf

[13] Brady, Mary. TGDC Meeting. National Institute of Standards and Technology (April 2019). *VVSG 2.0 Update*. Retrieved from https://www.eac.gov/events/2019/09/19/tgdc-meeting-september-19--20-2019-technical-guidelines-development-committee-tgdc/

[14] Code of Virginia § 24.2-629, *State Board approval process of electronic voting systems.* Retrieved from https://law.lis.virginia.gov/vacode/title24.2/chapter6/section24.2-629/

[15] Code of Virginia § 24.2-629, *State Board approval process of electronic voting systems.* Retrieved from https://law.lis.virginia.gov/vacode/title24.2/chapter6/section24.2-629/

[16] Virginia Department of Elections. Agenda and Working Papers (September 2019) *Voting System Certification Standard*. Retrieved from https://townhall.virginia.gov/L/GetFile.cfm?File=Meeting\151\29240\Agenda_ELECT_29240_v3.pdf

[17] Virginia Department of Elections. Agenda and Working Papers (September 2019) *Voting System Certification Standard*. Retrieved from https://townhall.virginia.gov/L/GetFile.cfm?File=Meeting\151\29240\Agenda_ELECT_29240_v3.pdf

[18] D. Persico, personal communication at State Board of Elections meeting, Nov 2019.

[19] Virginia Department of Elections. Minutes (September 2019). Retrieved from https://www.townhall.virginia.gov/L/GetFile.cfm?File=Meeting\151\29240\Minutes_ELECT_29240_v4.pdf

[20] Virginia Department of Elections. Agenda and Working Papers (September 2019) *Voting System Certification Standard*. Retrieved from https://townhall.virginia.gov/L/GetFile.cfm?File=Meeting\151\29240\Agenda_ELECT_29240_v3.pdf

[21] Virginia Department of Elections (December 2019). *Electronic Pollbook Certification Standard (DRAFT)*. Retrieved from https://www.townhall.virginia.gov/L/meetings.cfm on 3 Dec. 2019; later postponed from the December agenda.

[22] League of Women Voters of the United States (LWVUS). (2018). Representative government. *Impact on Issues 2018-2020*, pp. 16. Retrieved from https://www.lwv.org/sites/default/files/2019-04/LWV 2018-20 Impact on Issues.pdf
[23] Brennan Center for Justice (201). Early Voting: What Works. Retrieved from https://www.brennancenter.org/sites/default/files/publications/VotingReport_Web.pdf
[24] Presidential Commission on Election Administration (January). The American Voting Experience. Retrieved from https://www.eac.gov/assets/1/6/Amer-Voting-Exper-final-draft-01-09-14-508.pdf
[25] Presidential Commission on Election Administration (January 2014). p. 56.
[26] Presidential Commission on Election Administration (January 2014). p. 56.
[27] Presidential Commission on Election Administration (January 2014). p. 56.
[28] National Conference of State Legislatures (11/7/2019). Absentee and Early Voting. Retrieved from http://www.ncsl.org/research/elections-and-campaigns/absentee-and-early-voting.aspx
[29] Virginia Public Access Project. Early Voting Visuals. Retrieved from https://www.vpap.org/visuals/tag/early-voting/.
[30] League of Women Voters-Fairfax Area (09/18/2018). Statement: League Supports No Excuse Absentee Voting. Retrieved from https://www.lwv-fairfax.org/advocacy
[31] Code of Virginia §24.2-701.1
[32] Virginia Legislative Information Service 2020, HB 1, SB 111.
[33] Virginia Legislative Information Service 2020, HB 207.
[34] Virginia State Board of Elections (11-12-2019). Absentee Voting Report, approved 11-18-2019, Board Minutes. Retrieved from https://townhall.virginia.gov/L/GetFile.cfm?File=Meeting\151\29242\Minutes_ELECT_29242_v2.pdf
[35] Included in enacted versions of HB 1 and SB 111. Virginia Legislative Information Service 2020.
[36] Included in enacted versions of HB 1 and SB 111. Virginia Legislative Information Service 2020.
[37] Included in enacted version of SB 617. Virginia Legislative Information Service 2020
[38] Included in enacted versions of HB 1 and SB 111. Virginia Legislative Information Service 2020.
[39] C Piper, ELECT Commissioner, individual interview, December 3, 2019.
[40] A. Robbins, personal communication, December 4, 2019
[41] G. Reinemeyer, personal communication, December 9, 2019
[42] W. Latham, personal communication, October 1, 2019
[43] D. Moorman, personal communication, October 1, 2019
[44] League of Women Voters of the United States (LWVUS). (2018). Representative government. *Impact on Issues 2018-2020*, p. 13. Retrieved from https://www.lwv.org/sites/default/files/2019-04/LWV 2018-20 Impact on Issues.pdf
[45] League of Women Voters of Virginia (LWV-VA). (2019, Spring). *Positioned for Action,* p. 4. https://lwv-va.org/wp-content/uploads/2019/06/lwv-va-positions-Full-2019-Final-6-2-19.pdf
[46] U.S. Election Assistance Commission (June 25, 2018). Risk-Limiting Audits – Practical Application, p. 3. Retrieved from https://www.eac.gov/sites/default/files/eac_assets/1/6/Risk-Limiting_Audits_-_Practical_Application_Jerome_Lovato.pdf
[47] Satija, N., Gardner, A., & Marks, J., "Fears Persist as Ga. Debuts New Voting Machines ." (2019 December 24). Washington Post, p. A4.
[48] U.S. Election Assistance Commission, Blog, Defining and Piloting Risk Limiting Audits (August 9, 2018). Retrieved from https://www.eac.gov/defining-and-piloting-risk-limiting-audits
[49] See generally, "Principles and Best Practices for Post-Election Tabulation Audits," (December 2018). Retrieved from http://electionaudits.org/files/best%20practices%20final_0.pdf
[50] Washington Post, Opinion, A simple step every state could take to safeguard elections (October 21, 2019). Retrieved from https://www.washingtonpost.com/opinions/election-security-that-mitch-mcconnell-should-get-behind/2019/10/21/319eec70-f1d7-11e9-8693-f487e46784aa_story.html
[51] U.S. Election Assistance Commission, Blog, Defining and Piloting Risk Limiting Audits (August 9, 2018). Retrieved from https://www.eac.gov/defining-and-piloting-risk-limiting-audits
[52] National Conference of State Legislatures. "Post Election Audits." (2019 October 25). Retrieved from: https://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx
[53] U.S Election Assistance Commission, Grant Expenditure Report, Fiscal Year 2018 (April 4, 2019), pp. 10-15. Retrieved from https://www.eac.gov/sites/default/files/eac_assets/1/6/FY2018HAVAGrantsExpenditureReport.pdf

[54] *E.g.*, Brennan Center for Justice, Common Cause, Microsoft, National Election Defense Council, and Verified Voting, "Making Every Vote Count: A Practical Guide to Risk-Limiting Audits," seminar live-streamed on January 31, 2019 (YouTube).
[55] Bollinger, L., McRobbie, M. (2018 September 8). Securing the Vote: Protecting American Democracy. Washington, D.C., National Academies Press, p. 101.
[56] Virginia State Board of Elections, Agenda (December 18, 2019) pp 36-38. Retrieved from https://townhall.virginia.gov/L/GetFile.cfm?File=Meeting\151\29243\Agenda_ELECT_29243_v6.pdf
[57] Virginia State Board of Elections, Minutes (December 18, 2019), lines 69-79. Retrieved from https://townhall.virginia.gov/L/GetFile.cfm?File=Meeting\151\29243\Minutes_ELECT_29243_v1.pdf
[58] Virginia State Board of Elections, Agenda. (2019 December 18) p. 36.
[59] Reinemeyer, G., personal communication (December 9, 2019), and Robbins, A., personal communication, (December 4, 2019)
[60] League of Women Voters of the United States (LWVUS). (2018). Representative government. *Impact on Issues 2018-2020*, p.11. Retrieved from https://www.lwv.org/sites/default/files/2019-04/LWV 2018-20 Impact on Issues.pdf
[61] League of Women Voters of the United States (LWVUS). (2018). Representative government. *Impact on Issues 2018-2020*, p. 16. Retrieved from https://www.lwv.org/sites/default/files/2019-04/LWV 2018-20 Impact on Issues.pdf
[62] Johnson, Jeh. (January 6, 2017). *Statement by Secretary Jeh Johnson on the designation of election infrastructure as a critical infrastructure subsector*. Retrieved from https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical
[63] U. S. Senate Select Committee on Intelligence. (2019) p. 12
[64] Project on Government Oversight. (November 16, 2018) *Securing Our Elections: How States Can Mitigate the Potential Damage of Hacked Voter Registration Rolls*. Retrieved from https://www.pogo.org/report/2018/11/election-day-under-attack-how-states-can-mitigate-the-potential-damage-of-hacked-voter-registration-rolls/#heading-1
[65] CISA (November 15, 2019). *Security Tip (ST19-002) Best Practices for Securing Election Systems*. Retrieved from https://www.us-cert.gov/ncas/tips/ST19-002
[66] NIST Computer Security Resource Center. *The Cybersecurity Framework. New to Framework.* Retrieved from https://www.nist.gov/cyberframework/new-framework
[67] CISA *Security Tip (ST16-001)*.
[68] Center for Internet Security. (2018). *A Handbook for Elections Infrastructure Security*. p. 7. Retrieved from https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf
[69] CIS *MS-ISAC Multi-State Information Sharing & Analysis Center*. Retrieved from https://www.cisecurity.org/ms-isac/
[70] Virginia Department of Elections (August 20, 2019). *VERIS RFP Project, Fairfax County Site Visit and Interview Notes.* Retrieved from www.elections.virginia.gov/media/formswarehouse
[71] Joint Legislative Audit and Review Commission. *Recommendations and Options: Operations and Performance of Virginia's Department of Elections.* Retrieved from http://jlarc.virginia.gov/2018-elections.asp
[72] Piper, C. (2019, 3 Dec). Personal communication. Meeting between representatives of LWV-VA election study team and the Commissioner and Deputy Commissioner of Elections.
[73] Virginia Information Technologies Agency. *2018 Commonwealth of Virginia Information Security Report*. Retrieved from https://www.vita.virginia.gov/media/vitavirginiagov/commonwealth-security/pdf/2018-Commonwealth-of-Virginia-Information-Security-Annual-Report.pdf
[74] Virginia Department of Elections, *Annual List Maintenance Report September 1, 2018 – August 31, 2019*. Retrieved from https://www.elections.virginia.gov/media/formswarehouse/maintenance-reports/2019SBEListMaintenancereport.pdf
[75] Virginia Department of Elections, *VERIS RFP Locality Survey Results. Version 1.0 – 10/03/2019*. Retrieved from https://www.elections.virginia.gov/media/formswarehouse/veris-rfp-project/VERIS-RFP-Project-Locality-Survey-Results.pdf
[76] Virginia Department of Elections, *Election Night Reporting*. Retrieved from https://www.elections.virginia.gov/resultsreports/election-night-reporting/index.html
[77] CISA *Security Tip (ST16-001). Securing Voter Registration Data*. Retrieved from https://www.us-cert.gov/ncas/tips/ST16-001
[78] CIS Center for Internet Security. *A Handbook for Elections Infrastructure Security. Version 1.0 February 2018*, p. 12. Retrieved from https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

[79] Becker, David, Jacob Kipp, Jack R. Williams, and Jenny Lovell. Center for Election Innovation & Research (September 2018). *Voter Registration Database Security*, p. 15. Retrieved from https://electioninnovation.org/2018-vrdb-security/
[80] Code of Virginia. (2019) *Title 24.2-410.2 Security of the Virginia voter registration system*. Retrieved from https://law.lis.virginia.gov/vacode/title24.2/chapter4/section24.2-410.2/
[81] Virginia Department of Elections. News Release (November 18, 2019). *Virginia State Board of Elections Approves Election Security Standards for 2020*. Retrieved from https://www.elections.virginia.gov/new-releases/virginia-state-board-of-elections-approves-election-security-standards-for-2020.html
[82]Virginia Department of Elections. Letter to U. S. Election Assistance Commission: *2018 HAVA Budget Narrative*. [copy received from Commissioner of Elections]
[83] LWV-VA / R. Lawson (2019). Adapted from CIS Center for Internet Security. *A Handbook for Elections Infrastructure Security. Version 1.0 February 2018*, p.14. Retrieved from https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf
[84] Bowman, Jessica (December 18, 2019). Commissioner's Report to State Board of Elections.
[85] League of Women Voters of the United States (LWVUS). (2018). Representative government. *Impact on Issues 2018-2020*, p.11. Retrieved from https://www.lwv.org/sites/default/files/2019-04/LWV 2018-20 Impact on Issues.pdf
[86] League of Women Voters of the United States (LWVUS). (2018). Representative government. *Impact on Issues 2018-2020*, p. 13. Retrieved from https://www.lwv.org/sites/default/files/2019-04/LWV 2018-20 Impact on Issues.pdf
[87] CIS Center for Internet Security. *A Handbook for Elections Infrastructure Security.* Version 1.0 (2018, February), p.20. Retrieved from https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf
[88] The National Academies of Science, Engineering, and Medicine (2018)
[89] O'Sullivan, Dan, UpGuard blog (2019, Nov 20). *The Chicago Way: An Electronic Voting Firm Exposes 1.8M Chicagoans.* Retrieved from https://www.upguard.com/breaches/cloud-leak-chicago-voters
[90] Verified Voting. *Ballot Marking Devices*. Retrieved from https://www.verifiedvoting.org/ballot-marking-devices/
[91] Verified Voting. *Ballot Marking Devices*.
[92] Wilkie, Jordan. Carolina Public Press (2019, August 23). *NC certifies barcode ballot voting systems despite security concerns.* Retrieved from https://carolinapublicpress.org/29234/nc-certifies-barcode-ballot-voting-systems-despite-security-concerns/
[93] National Election Defense Coalition. *Vulnerable Voting Systems: Ballot Marking Devices*. Retrieved from https://www.electiondefense.org/ballot-marking-devices
[94] National Conference of State Legislatures (2018, Aug. 20). *Voting Equipment.* Retrieved from https://www.ncsl.org/research/elections-and-campaigns/voting-equipment.aspx
[95] Jones, Douglas W. The University of Iowa Department of Computer Science(2010). *On Optical Mark-Sense Scanning".* Retrieved from https://www.semanticscholar.org/paper/On-Optical-Mark-Sense-Scanning-Jones/32fc2e75d4bb7b920f2e16f15f6ff2d0e46ebb15
[96] U.S. Election Assistance Commission (2008, May). *Quick Start Guides: Central-Count Optical Scan Ballots*. Retrieved from https://www.eac.gov/election-officials/quick-start-guides
[97] Jones, Douglas W. NIST Workshop: Developing an Analysis of Threats to Voting Systems (2005, Sept. 5). *Example Attack Documentation*: *Optical Scan Configuration File*. Retrieved from https://www.nist.gov/system/files/documents/itl/vote/threatworksummary.pdf
[98] Cortés, E., Ramachandran, G., Howard, L., & Norden, L. (2019). *Preparing for Cyberattacks and Technical Failures: A Guide for Election Officials.* Brennan Center for Justice, New York University School of Law. Retrieved from https://www.brennancenter.org/sites/default/files/2019-12/2019_12_ContingencyPlanning.pdf.
[99] Center for Internet Security (2018)
[100] The National Academies of Sciences, Engineering, and Medicine (2018). *Securing the Vote: Protecting American Democracy.* Retrieved from https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy.
[101] Cortés, E., Ramachandran, G., Howard, L., & Norden, L. (2019).
[102] CIS Center for Internet Security (2018), pp.56-64.
[103] The National Academies of Sciences, Engineering, and Medicine (2018). *Securing the Vote: Protecting American Democracy.* p .6. Retrieved from https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy.

[104] Belfer Center for Science and International Affairs, Harvard Kennedy School. (2018, February). *The State and Local Election Cybersecurity Playbook.* Retrieved from https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook
[105] National Election Defense Coalition. Expert Letter to Congress, (2017, June 21). *Integrity in Elections.* Retrieved from https://www.electiondefense.org/election-integrity-expert-letter
[106] VerifiedVoting.org (November 2020). *The Verifier - Absentee Ballot Equipment in Virginia*. Retrieved from https://www.verifiedvoting.org/verifier/#year/2020/state/51
[107] Code of Virginia § 24.2-626.1. Acquisition and use of accessible voting devices.
[108] Code of Virginia § 24.2-626. (Effective July 1, 2020) Governing bodies shall acquire electronic voting systems.
[109] Code of Virginia §24.2-626
[110] ELECT presentation to State Board of Elections (SBE) on Voting System Certification Standards. SBE Working Papers, November 2019.
[111] LWV-VA / R. Lawson (2019). Adapted from CIS Center for Internet Security. *A Handbook for Elections Infrastructure Security.* Version 1.0 (2018, February), p.14. Retrieved from https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf
[112] Code of Virginia §24.2-629 (E)
[113] U. S. Election Assistance Commission. Election Management Guidelines. *Chapter 6: Pre-Election and Parallel Testing.* Retrieved from https://www.eac.gov/sites/default/files/eac_assets/1/6/Chapter_6__Pre-Election_and_Parallel_Testing.pdf
[114] Virginia Department of Elections (2019, September). *Voting System Certification Standard*. Retrieved from SBE Working Papers, September 2019. p 19.
[115] Code of Virginia §24.2-611(D)
[116] The Pew Charitable Trusts (2017). *A Look at How—and How Many—States Adopt Electronic Poll Books.* Retrieved from https://www.pewtrusts.org/en/research-and-analysis/data-visualizations/2017/a-look-at-how-and-how-many-states-adopt-electronic-poll-books.
[117] The Pew Charitable Trusts (2017)
[118] Code of Virginia §24.2-611(E)
[119] Root, D., Kennedy, L., Sozan, M., & Parshall, J. (2018). *Election Security in All 50 States: Defending America's Elections.* Center for American Progress. Retrieved from https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/.
[120] Virginia State Board of Elections (2015). *Electronic Pollbook Certification: Procedures & System Requirements.* Rev-0515. Retrieved from https://www.eac.gov/sites/default/files/eac_assets/1/28/Virginia%20EPB%20Certification%20Procedures%20and%20System%20Requirements%20REV-05151.pdf.
[121] Code of Virginia § 24.2-410.2. Security of the Virginia voter registration system.
[122] Virginia Department of Elections (2019, September). *Voting System Certification Standard*. Retrieved from SBE Working Papers, September 2019.
[123] League of Women Voters of the United States (LWVUS). (2018). Representative government. *Impact on Issues 2018-2020*, p.11. Retrieved from https://www.lwv.org/sites/default/files/2019-04/LWV 2018-20 Impact on Issues.pdf
[124] U.S. Election Assistance Commission. (2015). 2015 Voluntary Voting System Guidelines, Volume 1, Version1.1. Retrieved from https://www.eac.gov/assets/1/28/VVSG%201.1%20VOL%201.508compliant.FINAL.pdf
[125] U.S. Election Assistance Commission. (2015). 2015 Voluntary Voting System Guidelines, Volume 1, Version1.1. Retrieved from https://www.eac.gov/assets/1/28/VVSG%201.1%20VOL%201.508compliant.FINAL.pdf .
[126] League of Women Voters of the United States. Election Audit Task Force. (2009). "Report on Election Auditing". Washington, DC. Retrieved from https://www.lwv.org/sites/default/files/2018-07/report-electionaudits.pdf
[127] League of Women Voters Education Fund (LWVEF). (2004, July). Helping America vote: Safeguarding the vote, p. 7. Retrieved from https://www.lwv.org/expanding-voter-access/helping-america-vote-safeguarding-vote
[128] Norden, L. and Famighetti, C. (2015). *America's Voting Machines at Risk,* Brennan Center for Justice at New York University School of Law. New York, NY. p.7. Retrieved from https://www.brennancenter.org/our-work/research-reports/americas-voting-machines-risk

[129] Norden, L., DeLuzio, C. & Ramachandran, G. (2019). "A Framework for Vendor Election Oversight". Policy Report from Brennan Center for Justice at New York University School of Law. New York, NY. Retrieved from https://www.brennancenter.org/our-work/policy-solutions/framework-election-vendor-oversight.
[130] U.S. Election Assistance Commission (EAC). (2017b, September). Voluntary Voting Systems Guidelines 2.0 principles and guidelines, p.4. Retrieved from https://www.eac.gov/assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf
[131] Virginia Legislative Information Service, Retrieved from https://lis.virginia.gov.
[132] National Conference of State Legislatures. (2018). *Voting system standards, testing and certification.* Retrieved from http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx
[133] Code of Virginia. (2018). Title 24.2 Elections. Chapter 6. The election. Retrieved from https://law.lis.virginia.gov/vacode/
[134] Code of Virginia. § 24.2-625.1
[135] Piper,C. personal communication, December 3, 2019
[136] Piper, C. (2018, July 16). Virginia Narrative Budget. Letter to Mark Abbott, U.S. Election Assistance Commission. July 16. Retrieved from https://www.eac.gov/havadocuments/VA_Narrative_Budget.pdf
[137] Jacobs, M. (2019, September 20). The cybersecurity 202: McConnell's support for election security funding is just the start of a big fight. *The Washington Post.* Retrieved from https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/09/20/the-cybersecurity-202-mcconnell-s-support-for-election-security-funding-is-just-the-start-of-a-big-fight/5d83e2a5602ff1737aef7323/
[138] Virginia State Department of Elections. (2019, November 18). *Virginia State Board of Elections approves standards for 2020* [Press release] Retrieved from https://www.elections.virginia.gov/new-releases/virginia-state-board-of-elections-approves-election-security-standards-for-2020.html
[139] Interview with Christopher E. Piper, Commissioner of the Department of Elections, December 3, 2019.
[140] Persico, D. (November 18, 2019). HB2178 minimum security standards. Working paper in Agenda, Virginia Department of Elections, pp. 72-129. Retrieved from https://townhall.virginia.gov/l/GetFile.cfm?File=meeting%5C151%5C29242%5CAgenda_ELECT_29242_v2.pdf
[141] League of Women Voters of the United States (LWVUS). (2018). Representative government. *Impact on Issues 2018-2020*, p.11. Retrieved from https://www.lwv.org/sites/default/files/2019-04/LWV 2018-20 Impact on Issues.pdf
[142] National Academies of Science, Engineering, and Medicine, 2018. "Securing the Vote: Protecting American Democracy." Washington, DC: The National Academies Press. Retrieved from https://doi.org/10.17226/25120.
[143] U.S. Election Assistance Commission. (2011 September) A Survey of Internet Voting. Washington, D.C.
[144] See Summary from National Conference of State Legislatures posted at https://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx.
[145] Fowler, A. (2019 July) Promises and Perils of Mobile Voting, p.8. Retrieved from https://cpb-us-w2.wpmucdn.com/web.sas.upenn.edu/dist/7/538/files/2019/06/Fowler_MobileVoting.pdf.
[146] Fowler, A. (2019 July) Promises and Perils of Mobile Voting, Retrieved from https://cpb-us-w2.wpmucdn.com/web.sas.upenn.edu/dist/7/538/files/2019/06/Fowler_MobileVoting.pdf.)
[147] Senti, F. (2019). *The Denver Mobile Voting Pilot: A Report*. Retrieved from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjF7PHIjJ3nAhUToZ4KHYCPDHEQFjAAegQIBBAB&url=https%3A%2F%2Fcyber-center.org%2Fwp-content%2Fuploads%2F2019%2F08%2FMobile-Voting-Audit-Report-on-the-Denver-County-Pilots-FINAL.pdf&usg=AOvVaw3xr3WU0lWDe6puVQXt1hgG
[148] Department of Defense/Federal Voting Assistance Program. (2018) Report to Congress. p.36. Washington, DC: Retrieved from https://www.fvap.gov/uploads/FVAP/Reports/RTC_20190531(Final).pdf.
[149] Department of Defense/Federal Voting Assistance Program. (2018) Report to Congress. Washington, DC: Retrieved from https://www.fvap.gov/uploads/FVAP/Reports/RTC_20190531(Final).pdf.
[150] A number of states allow UOCAVA voters to submit their ballots electronically. For more information, *see* http://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx.
[151] Department of Defense/Federal Voting Assistance Program. (2018) Report to Congress. Washington, DC: Retrieved from https://www.fvap.gov/uploads/FVAP/Reports/RTC_20190531(Final).pdf.
[152] Abrams, A. (2019, Nov. 4) Smartphone Voting Could Expand Accessibility, But Election Experts Raise Security Concerns, Time, Retrieved from https://time.com/5717479/mobile-voting-accessibility/.

[153] Government Accountability Office. (2017 Dec. 4). Voters With Disabilities: Observations on Polling Place Accessibility and Related Federal Guidance. (GAO Publication 18-4) Washington, D.C.: U.S. Government Printing Office.
[154] Solaiman, I. (Nov. 2018) Defending Vote Casting: Using Blockchain-Based Mobile Voting Applications in Government Elections. p.11-14 Retrieved from https://www.belfercenter.org/publication/defending-vote-casting-using-blockchain-based-mobile-voting-applications-government
[155]Verified Voting, 2019, "Internet Voting is Not Secure for Any Voter" (two-page handout);
[156] Greenhalgh, S., Goodman, S., Rosenzweig, P., Epstein, J., (2018), "Email and Internet Voting: The Overlooked Threat to Election Security," pp. 10. Retrieved from https://www.commoncause.org/page/email-and-internet-voting-the-overlooked-threat-to-election-security/.
[157] Dill, D. (and 31 others), (2008). "Computer Technologists' Statement on Internet Voting." Retrieved from https://verifiedvoting.org/resources/internet-voting, p.1.
[158] National Academies of Science, Engineering, and Medicine, 2018. "Securing the Vote: Protecting American Democracy." Washington, DC: The National Academies Press. p. 103. Retrieved from https://doi.org/10.17226/25120.
[159] Jefferson, D., (2019). Verified Voting. "If I Can Shop and Bank Online, Why Can't I Vote Online?", p. 5. Retrieved from https://www.verifiedvoting.org/resources/internet-voting/vote-online/
[160] Greenhalgh, S., Goodman, S., Rosenzweig, P., Epstein, J. (2018), (Email and Internet Voting: The Overlooked Threat to Election Security, p.8.
[161] Greenhalgh, S., Goodman, S., Rosenzweig, P., Epstein, J., (2018), "Email and Internet Voting: The Overlooked Threat to Election Security," pp. 13. Retrieved from https://www.commoncause.org/page/email-and-internet-voting-the-overlooked-threat-to-election-security/
[162] National Academies of Science, Engineering, and Medicine, 2018. "Securing the Vote: Protecting American Democracy." Washington, DC: The National Academies Press. p. 105-6. Retrieved from https://doi.org/10.17226/25120.
[163] Kiniry, J., Zimmerman, D., Wagner, D., Robinson, P., Foltzer, A. Morina, S., 2015. "The Future of Voting," U.S. Vote Foundation. p. iv. Retrieved from https://www.usvotefoundation.org/E2E-VIV.
[164] Greenhalgh, S., Goodman, S., Rosenzweig, P., Epstein, J., (2018), "Email and Internet Voting: The Overlooked Threat to Election Security," pp. 13. Retrieved from https://www.commoncause.org/page/email-and-internet-voting-the-overlooked-threat-to-election-security/
[165] Wolchok, S., Wustrow, E., Isabel, D., & Halderman, J.A. (2012 February). "Attacking the Washington,D.C. Internet Voting System." *Proceedings, 16th Conference on Financial Cryptography & Data Security.*
[166] Halderman, J.A., Remarks at Election Verification Network Conference, Washington, D.C., (2019 March 3).
[167] Piper, C. (2019 December). Personal interview.
[168] National Academies of Science, Engineering, and Medicine, 2018. "Securing the Vote: Protecting American Democracy." Washington, DC: The National Academies Press. p. 102. Retrieved from https://doi.org/10.17226/25120.
[169] E.g., SB 11 (2014), HB 759 (2014), HB 237 (2016), SB 559 (2018), and HB 2588 (2019). https://lis.virginia.gov/cgi-bin/legp604.exe?191+men+BIL. A bill before the 2020 session of the Virginia General Assembly, HJ23, would mandate a study of blockchain for remote voting.
[170] Virginia Department of Elections, 2015. "SB 11 Workgroup Report: Building a Secure Electronic Return of Marked Ballots Solution for our Overseas Military Voters."
[171] Virginia Department of Elections, & SB 11 Workgroup Report. (2015). *Building a Secure Electronic Return of Marked Ballots Solution for our Overseas Military Voters*. Retrieved from https://www.elections.virginia.gov/.../SB11Draft11-16-2015MeetingInput.pdf
[172] Epstein, J., (2019 December). Personal interview. Note that Epstein is also an author of the definitively negative assessment "Email and Internet Voting: The Overlooked Threat to Election Security," referenced in endnote 8 above.
[173] HB 238, SB 455, HB 239,Virginia Legislative Information System, 2020 Session.
[174] League of Women Voters of the United States (LWVUS). (2018). Representative government. *Impact on Issues 2018-2020*, p.11. Retrieved from https://www.lwv.org/sites/default/files/2019-04/LWV 2018-20 Impact on Issues.pdf
[175] League of Women Voters of Virginia (LWV-VA). (2019, Spring). *Positioned for Action,* p. 4. https://lwv-va.org/wp-content/uploads/2019/06/lwv-va-positions-Full-2019-Final-6-2-19.pdf
[176] Therese Martin, personal communication, January 1, 2020

[177] Olga Hernandez, personal communication, January 2, 2020
[178] SB 1256. (2013). SB 1356 Voter identification requirements; photo ID required at polls, application for absentee ballot. Virginia Legislative Information Service. 2013 Session. Retrieved from http://lis.virginia.gov/cgi-bin/legp604.exe?131+sum+SB1256S
[179] § 24.2-404 of the Virginia Code. Retrieved from https://law.lis.virginia.gov/vacode/title24.2/chapter6/section24.2-404/
[180] Wilson, R. (2013, November 5). Five reasons voter identification bills disproportionally impact women. *The Washington Post.* Retrieved from https://www.washingtonpost.com/blogs/govbeat/wp/2013/11/05/five-reasons-voter-identification-bills-disproportionately-impact-women/
[181] Opsal, E. (2014, November 7). Media wrap up: How voters fared with new restrictions. Brennan Center for Justice at New York University School of Law. Retrieved from https://www.brennancenter.org/our-work/analysis-opinion/mehttps://www.brennancenter.org/our-work/analysis-opinion/media-wrap-how-voters-fared-new-restrictionsdia-wrap-how-voters-fared-new-restrictions
[182] Virginia Department of Elections. (2019). Results/reports. Estimated provisional counts. Statistics. Retrieved from https://results.elections.virginia.gov/vaelections/2019 November General/Site/Statistics/ProvisionalCounts.html
[183] Marrimow, A.E. and Weiner, R. (2016, December 13). Appeals court upholds Virginia's voter-ID law. *The Washington Post.* Retrieved from https://www.washingtonpost.com/local/public-safety/appeals-court-upholds-virginias-voter-id-law/2016/12/13/3888f46e-c150-11e6-9a51-cd56ea1c2bb7_story.html
[184] Green, F. (2016, March 1). Former election officials testify that no Va. Voters denied due to photo ID law. Richmond Times-Dispatch. Retrieved from https://www.richmond.com/news/former-election-officials-testify-that-no-va-voters-denied-due/article_5a603fe5-7a08-504b-b2c7-257915ae6d42.html
[185] Lee v. Virginia Board of Elections. (2016). 843F.3d. 592. 4th Cir. Retrieved from https://casetext.com/case/lee-v-va-state-bd-of-elections-8
[186] HB 19 Voter identification; repeal of photo identification requirements. Virginia Legislative Information System, 2020 Session. Retrieved from http://lis.virginia.gov/cgi-bin/legp604.exe?ses=201&typ=bil&val=hb19
[187] SB 65 Voter identification; repeal of photo identification requirements. Virginia Legislative Information System, 2020 Session. Retrieved from http://lis.virginia.gov/cgi-bin/legp604.exe?ses=201&typ=bil&val=sb65
[188] SB 113 (2019, December 13). Voter identification; repeal of photo identification requirements. Virginia Legislative Information System Full Text, p. 5 Retrieved from https://lis.virginia.gov/cgi-bin/legp604.exe?201+ful+SB113+pdf
[189] League of Women Voters of the United States (LWVUS). (2018). Representative government. *Impact on Issues 2018-2020*, p. 13. Retrieved from https://www.lwv.org/sites/default/files/2019-04/LWV 2018-20 Impact on Issues.pdf