University of Pittsburgh

THE BLUE RIBBON COMMISSION ON PENNSYLVANIA'S ELECTION SECURITY

STUDY AND RECOMMENDATIONS

PITT CYBER

University of Pittsburgh Institute for Cyber Law, Policy, and Security

Contents

Introduction from the Co-Chairs

This report, and the work of the commission in preparing it, offers a thorough review of the cybersecurity of Pennsylvania's election architecture and the challenges we must take on to improve it.

From the colonial era through today, America has prided itself on its democratic ideals. Popular sovereignty—the essential right to choose one's own leaders through the ballot box—is central to this identity. The nation has greatly expanded the franchise over the years through a series of historical movements—often difficult and even violent. Pennsylvania has played an outsize role in that steady march of history, from Quaker meeting houses; to the Continental Congresses and the Constitutional Convention; to the Women's Suffrage, Labor, and Civil Rights movements.

In recent years, however, debates over the nation's elections have been less about the expansion of the franchise than about our capacity to conduct the vote fairly, efficiently, and securely. This should trouble all Americans. The health and success of our democracy depend in large measure on broad public trust in the execution of our representative form of government. Indeed, it is far easier to lose faith in the results of elections than it is to earn it.

Interference by foreign actors threatens this faith. There is a growing understanding that foreign propaganda and disinformation via social media by nation-state actors have introduced another type of threat to the credibility of our elections and, indeed, to our national discourse. No one should doubt these well-documented attempts at interference.

Although there have been dramatic improvements in American election security since 2016, more must be done—at the local, state, and federal levels.

We have little doubt that foreign adversaries will increase their efforts in the lead-up to the presidential election in 2020. The persistence and sophistication of these actors are only increasing.

Pennsylvanians in particular should be concerned about election security. Our state is one of the most vulnerable to election manipulation, in large part because of reliance on older electronic voting systems. As recently as the 2018 election, an estimated 83 percent of Pennsylvanians were voting on machines that offer no auditable paper record. This could thwart Pennsylvania's counties from detecting a successful hack, or even benign error, and it prevents counties from recovering in the instance of an attack.

Of course, it is not just the voting machines and closely linked election management systems that are at risk. There are multiple threat vectors throughout our election architecture, including in our voter registration system, tallying methods, and election-night reporting. The architecture is complex and was not built to withstand threats from nation-states and other sophisticated attackers.

Private election vendors play an outsize role in many Pennsylvania counties' election efforts. For many, unfortunately, we fear that security is far from a top priority.

And, as we are learning every day, even successful defense against attacks on the *outcome* of the vote may not be enough to protect Americans' faith in our elections. Any number of attacks could create chaos or confusion among poll workers and voters,

leading to a damaging loss of faith in election results, even where those results are not maliciously altered. A nation-state rival does not need to alter actual votes if Americans do not trust the vote tally.

The litany of threats is long—and exacerbated by a lack of funding and training for election officials, who are suddenly expected to be front-line cyber warriors defending our democracy against sophisticated nation-state actors.

However, we are heartened by an overwhelming consensus of experts about the way forward. From the National Academies of Sciences, Engineering, and Medicine and the U.S. Senate Intelligence Committee to hundreds of cybersecurity experts, the key remedies are clear: Use voting systems with voter-marked paper ballots; improve cybersecurity of election management and voter registration systems; conduct robust post-election audits; and have good contingency planning in place. These recommendations, and more, are detailed in the pages that follow.

The Governor's and Department of State's efforts to require counties to have voting systems with voter-verifiable paper records by the end of 2019 should reassure all Pennsylvanians. We urge the General Assembly to work closely with counties to fund these critical replacements. We must support our local election officials and the critical efforts by the Department of State to improve the Commonwealth's entire election architecture.

We must not pretend that the existing election architecture from an era of flip phones is sufficient to withstand a determined foreign adversary. Improving it will require political will, including funding. And it will require that the Commonwealth and counties be prepared to administer an election even in the face of a cyberattack.

This is not a partisan issue. And there is no question that Pennsylvania can—and must—secure its elections for our citizens.

This report, and the work of the commission in preparing it, offers a thorough review of the cybersecurity of Pennsylvania's election architecture and the challenges we must take on to improve it. We must be better prepared to manage the kinds of cyber threats that have targeted us in the past—and anticipate the threats of the future.

We are confident that this report offers evidence-based, actionable recommendations to secure Pennsylvania's elections. We hope that it might also serve as a model for other states in their own important efforts.

We, as Americans, must address our election security with the urgency the threat deserves.

David J. Hickton
Founding Director,
University of Pittsburgh Institute
for Cyber Law, Policy, and Security

Paul J. McNulty
President,
Grove City College

Acknowledgments

With support from:

THE HEINZ ENDOWMENTS
HOWARD HEINZ ENDOWMENT
VIRA I. HEINZ ENDOWMENT

THE PITTSBURGH FOUNDATION

PITT CYBER
University of Pittsburgh Institute for Cyber Law, Policy, and Security

in partnership with:

verifiedvoting

The University of Pittsburgh Institute for Cyber Law, Policy, and Security (Pitt Cyber) and The Blue Ribbon Commission on Pennsylvania's Election Security gratefully acknowledge the generous support of The Heinz Endowments and The Pittsburgh Foundation's Charles H. Spang Fund to host The Blue Ribbon Commission on Pennsylvania's Election Security.

The commission thanks Christopher Deluzio for his tremendous contribution to this report and throughout this entire effort; Beth Schwanke for her guidance and development of the commission; and the entire staff of Pitt Cyber, including Sarah Barca, Kate Ulreich, and Ray Winstead, for their contributions.

We are also grateful to the exceptional partnership and thoughtful expertise provided by Verified Voting throughout this effort.

Many thanks to Carnegie Mellon University's Software Engineering Institute for providing technical advice. Thanks to Jones Day for pro bono support, especially David Coogan, as well as the many individuals at the University of Pittsburgh and beyond without whom this project could have never occurred.

We are sincerely grateful for all of the cooperation from Kathy Boockvar, senior adviser to the governor on election modernization (and, as of January 4, 2019, slated for nomination as secretary of the commonwealth); Jonathan Marks, commissioner, Bureau of Commissions, Elections, and Legislation, Department of State; Tim Benyo, chair, Association of Eastern Pennsylvania County Election Personnel; Shari Brewer, chair, Western Pennsylvania Election Personnel Association; and Ed Allison, director of voter registration, Lawrence County.

We acknowledge all of the thoughtful contributions we received in public comments and the many organizations and people throughout Pennsylvania and the country who provided us with their expertise and insight. In particular, thanks to those who presented at the commission's meetings, including state and county election personnel; J. Alex Halderman, professor of computer science, University of Michigan; and Elizabeth Howard, counsel, Brennan Center for Justice.

Commission Members*

SENIOR ADVISORS

Charlie Dent: former U.S. congressman, 15th District of Pennsylvania

Paul H. O'Neill: 72nd Secretary of the U.S. Treasury

Dick Thornburgh: Former governor, Pennsylvania; former Attorney General of the United States; former Under-Secretary-General of the United Nations

David Hickton: founding director, Pitt Cyber; former U.S. Attorney for the Western District of Pennsylvania (co-chair)

Paul McNulty: president, Grove City College; former Deputy Attorney General of the United States; former U.S. Attorney for the Eastern District of Virginia (co-chair)

Jim Brown: former chief of staff to U.S. Senator Robert P. Casey Jr.; former chief of staff to Pennsylvania Governor Robert P. Casey

Esther L. Bush: president and CEO, Urban League of Greater Pittsburgh

Mary Ellen Callahan: former chief privacy officer, U.S. Department of Homeland Security

Susan Carty: president, League of Women Voters of Pennsylvania

Nelson A. Diaz: retired judge, Philadelphia Court of Common Pleas

Jane Earll: attorney; former Pennsylvania senator

Douglas E. Hill: executive director, County Commissioners Association of Pennsylvania

Mark A. Holman: partner, Ridge Policy Group; former deputy assistant to the president for Homeland Security; former chief of staff to Pennsylvania Governor Tom Ridge

Ken Lawrence: vice chair, Montgomery County Board of Commissioners

Mark A. Nordenberg: chair of the Institute of Politics, University of Pittsburgh; Chancellor Emeritus of the University; Distinguished Service Professor of Law

Grant Oliphant: president, The Heinz Endowments

Pedro A. Ramos: president and CEO, The Philadelphia Foundation

James C. Roddey: former chief executive, Allegheny County

Marian K. Schneider: president, Verified Voting; former Pennsylvania Deputy Department of State for Elections and Administration

Bobbie Stempfley: director, CERT Division, Software Engineering Institute, Carnegie Mellon University

David Thornburgh: president and CEO, Committee of Seventy

Sharon Werner: former chief of staff to U.S. Attorneys General Eric H. Holder Jr. and Loretta E. Lynch

Dennis Yablonsky: former CEO, Allegheny Conference on Community Development; former Pennsylvania Secretary of Community and Economic Development

* Affiliations are provided for identification purposes. Commissioners are serving in their personal capacities.

Executive Summary**

** Campaigns & election infrastructure is in a period of significant change. The commission has strived to provide the most accurate and up-to-date information. For publication purposes, this report reflects information current as of January 4, 2019 unless otherwise noted.

These threats strike at the heart of democracy in Pennsylvania and throughout the United States. Securing our elections is not a partisan issue—and Pennsylvanians of every political persuasion should embrace the solutions that the commission recommends.

ELECTION INFRASTRUCTURE THROUGHOUT THE COUNTRY IS UNDER THREAT—AND PENNSYLVANIA IS NO EXCEPTION.

In fact, Pennsylvania's elections are worryingly susceptible to hacking for two primary reasons. First, the Commonwealth is a regular battleground state, with tight presidential election results, close congressional elections, and myriad other hotly contested races, making it an appealing target for those wishing to wreak havoc on the United States and its democracy.

Second, the bulk of Pennsylvania's voting machines are vulnerable to hacking and manipulation, something that computer scientists have demonstrated for several years.[1] This vulnerability stems from many counties' use of insecure electronic voting systems that are susceptible to manipulation and offer no paper record—and therefore no way of verifying the tabulation of votes when the veracity of election results is questioned.

Given the clear and present danger that these paperless machines pose, replacing the systems with those that employ voter-marked paper ballots should be the most pressing priority for Pennsylvania officials to secure the Commonwealth's elections.

Yet because even the most secure voting machines are still at some risk for hacking, replacing the vulnerable paperless voting systems would be insufficient if not coupled with robust, post-election audits. Such audits, if conducted properly after every election, can ensure that officials are able to detect machine tabulation errors that might affect the outcomes of elections. Pennsylvania's Election Code does require some post-election tabulation auditing (a flat-rate audit); however, only counties that use paper ballots can meaningfully comply with the Election Code's requirements. Moreover, Pennsylvania officials should improve upon the Election Code by embracing risk-limiting audits, which would offer a more effective and efficient method of verifying election results.

Voter registration databases are also a target for cyberattack. According to federal officials, Russian operatives targeted several states' voter registration databases—including Pennsylvania's—in the lead-up to the 2016 presidential election. Pennsylvania's voter registration system, which is into its second decade of service, has several vulnerabilities that could expose the system to manipulation by hackers seeking to delete, alter, or create registration records.

Fortunately, Pennsylvania officials are poised to embark upon the procurement process to replace this system—a process that will present an opportunity to deploy best practices in selecting and managing election vendors. These private companies also service much of Pennsylvania's election architecture beyond the voter registration system and, if not managed properly, can introduce substantial vulnerabilities through lax cybersecurity practices and opaque supply chains.

Any cyber defense would be incomplete without strong and extensive contingency planning. Such measures—which run the gamut of having adequate backup paper supplies for electronic pollbooks, ensuring poll workers are trained to handle contingencies, and preparing for natural disasters and attacks on the electric grid—ensure that election systems can recover in the face of an attack or technological error. Thus, proper contingency planning can provide a measure of resilience, something that Pennsylvania could improve, particularly while many counties continue to use vulnerable paperless voting systems.

These threats strike at the heart of democracy in Pennsylvania and throughout the United States. Securing our elections is not a partisan issue—and Pennsylvanians of every political persuasion should embrace the solutions that the commission recommends.

It is impossible to eliminate completely the risk of cyberattack on Pennsylvania's election architecture. However, trust in the integrity of our elections hangs in the balance; Pennsylvania officials must work to both reduce the potential for attacks and mitigate the impact in the event of an attack or other technological event. Citizens' faith in democracy demands nothing less.

SUMMARY OF RECOMMENDATIONS

Recommendation 1: Replace Vulnerable Voting Machines with Systems Using Voter-Marked Paper Ballots.

Counties using direct recording electronic (DRE) systems should replace them with systems using voter-marked paper ballots (either by hand or by machine) before 2020 and preferably for the November 2019 election, as directed by the Pennsylvania Department of State.

The Department of State should decertify DRE voting systems following December 31, 2019, if not sooner.

The Department of State should not certify and counties should not procure DRE machines—not even with voter-verifiable paper audit trails—but instead systems that tabulate voter-marked paper ballots, which are retained for recounts and audits.

Recommendation 2: The Pennsylvania General Assembly and the Federal Government Should Help Counties Purchase Secure Voting Systems.

Pennsylvanians, including public officials, must recognize that election security infrastructure requires regular investments and upgrades. Our elections—and Pennsylvanians' faith in them—are not free.

The General Assembly should appropriate funding to help cover the cost of counties' purchase of voting systems that incorporate voter-marked paper ballots (marked either by hand or by ballot-marking device) and other needed improvements to Pennsylvania's election security.

The U.S. Congress should provide additional appropriations for states, like Pennsylvania, which need to replace significant numbers of DREs without voter-verifiable paper audit trails.

Pennsylvanians should support federal legislation that includes assistance for states to replace aging voting systems.

The Governor, General Assembly, and counties should explore creative financing mechanisms (such as a bond issuance) to assist counties with procuring more secure electronic voting systems with voter-marked paper records.

The General Assembly should also consider creating a fund for regular future appropriations as upgrades in security and accessibility technologies merit.

Review and, where not already in place, implement cybersecurity best practices across Pennsylvania's election architecture.

Recommendation 3: Implement Cybersecurity Best Practices throughout Pennsylvania's Election Architecture.

Ensure that vote-tallying systems: (1) are single-use systems; (2) are air-gapped; and (3) follow the one-way, one-use removable media rule. Have redundancies in reporting tallies.

Require counties to compare and reconcile precinct totals with countywide results to ensure that vote totals add up correctly.

The State and counties should be conscious of supply chain vulnerabilities. Any contractors or vendors should be assessed for security risks. Security considerations should be a key selection factor—not reviewed after a procurement decision has been reached.

Implement multifactor authentication before implementing changes to a registration record in SURE.

Add an additional layer of encryption to SURE system data.

Send paper notifications to registered voters after online changes to records.

Require mandatory pre-election testing of e-pollbooks across Pennsylvania (where e-pollbooks are used) to ensure e-pollbooks are in good and proper working order before Election Day.

Recommendation 4: Provide Cybersecurity Awareness Training for State and Local Election Officials.

The Commonwealth should continue to conduct cybersecurity training for state personnel. In addition, the Department of State should continue to work toward rolling out, in consultation with counties, cybersecurity training for local election officials throughout Pennsylvania.

Local officials should support Commonwealth efforts to roll out cybersecurity training and creatively look to leverage existing resources to ensure personnel are adequately prepared to face today's cybersecurity threats.

The Department of State should encourage local election officials to take advantage of federal cybersecurity training resources, such as the Department of Homeland Security's free, online, on-demand cybersecurity training system for governmental personnel and the inter-agency National Institute for Cybersecurity Careers and Studies.

Recommendation 5: Conduct Cybersecurity Assessments at the State and County Levels.

The Pennsylvania Department of State should continue to conduct, and all of Pennsylvania's counties should conduct, comprehensive cybersecurity assessments. Election officials should also conduct regular process audits across the election ecosystem.

Local officials should not only support but also work closely with Commonwealth officials in connection with cybersecurity assessments.

Election officials should avail themselves of the no-cost cybersecurity assessment resources offered by the U.S. Department of Homeland Security.

Pennsylvanians should support federal legislation that strengthens and supports federal cybersecurity resources and provides training and assessment assistance to state and local election officials.

The General Assembly should provide funding support to counties to implement regular, periodic cybersecurity assessments and audits, especially relating to election infrastructure.

Recommendation 6: Follow Vendor Selection Best Practices in SURE Replacement Procurement and Leverage Auditor General's Findings.

In connection with the upcoming procurement process to replace SURE, the Department of State should heed vendor selection best practices applicable to election infrastructure.

Beyond the SURE procurement process, the State and counties should be conscious of supply chain vulnerabilities.

The Department of State should work closely with the Auditor General's office in connection with that office's audit of Pennsylvania's voter registration system. Any relevant audit findings should be taken into account in the upcoming procurement process.

Recommendation 7: Employ Risk-Limiting Audits

Pennsylvania should employ transparent risk-limiting audits after each election.

The Department of State, in partnership with select counties, should pilot risk-limiting audits. The General Assembly should then pass legislation to make this a statewide requirement.

Recommendation 8: Implement Best Practices throughout Pennsylvania's Cyber Incident Response Planning.

Review and, where not already in place, incorporate cybersecurity best practices into Pennsylvania's cyber incident response plans.

All Pennsylvania counties should join the EI-ISAC (Elections Infrastructure-Information Sharing and Analysis Center).

The Pennsylvania Auditor General's audit and the Commonwealth's Inter-Agency Election Preparedness and Security Workgroup should examine cyber incident response plans.

The General Assembly should provide funding support to counties to bolster election-related contingency planning measures as part of a broader appropriation to support improvements to election security across the Commonwealth.

Recommendation 9: Revise the Election Code to Address Suspension or Extension of Elections Due to an Emergency.

The Election Code should provide clear authority for the suspension or extension of elections due to a wide-scale cyber-related attack, natural disaster, or other emergency that disrupts voting. The Election Code should include straightforward procedures governing the declaration of an emergency and the suspension or extension of voting.

Recommendation 10: Bolster Measures Designed to Address Voting Equipment–Related Issues So Voting Can Continue Even in the Event of Equipment Failure.

Ensure that emergency paper ballots sufficient for two to three hours of peak voting are available in every polling place using DRE machines.

Update poll worker training to address procedures for voting equipment failures.

Ensure that procedures are in place to ensure that voters with disabilities will be able to vote in the event of accessible voting equipment failures.

Recommendation 11: Enhance Measures Designed to Address E-pollbook–Related Issues So Voting Can Continue Even in the Event of Equipment Failure.

Ensure that provisional ballot materials sufficient for two to three hours of peak voting are available in every polling place using e-pollbooks.

Update poll worker training to address procedures for e-pollbook failures.

Counties using e-pollbooks should review and, where appropriate, implement cybersecurity best practices for e-pollbooks.

TABLE OF RECOMMENDATIONS BY RESPONSIBLE OFFICIAL

	State Officials	Local Officials	Federal Officials
Recommendation 1: Replace Vulnerable Voting Machines with Systems Using Voter-Marked Paper Ballots.	X	X	
Recommendation 2: The Pennsylvania General Assembly and the Federal Government Should Help Counties Purchase Secure Voting Systems.	X	X	X
Recommendation 3: Implement Cybersecurity Best Practices throughout Pennsylvania's Election Architecture.	X	X	
Recommendation 4: Provide Cybersecurity Awareness Training for State and Local Election Officials.	X	X	
Recommendation 5: Conduct Cybersecurity Assessments at the State and County Levels.	X	X	
Recommendation 6: Follow Vendor Selection Best Practices in SURE Replacement Procurement and Leverage Auditor General's Findings.	X	X	
Recommendation 7: Employ Risk-Limiting Audits.	X	X	
Recommendation 8: Implement Best Practices throughout Pennsylvania's Cyber Incident Response Planning.	X	X	X
Recommendation 9: Revise the Election Code to Address Suspension or Extension of Elections Due to an Emergency.	X		
Recommendation 10: Bolster Measures Designed to Address Voting Equipment–Related Issues So Voting Can Continue Even in the Event of Equipment Failure.	X	X	
Recommendation 11: Enhance Measures Designed to Address E-pollbook–Related Issues So Voting Can Continue Even in the Event of Equipment Failure.	X	X	

Voting and Election Management Systems

Overview

It is imperative that officials take steps to address these vulnerabilities before the 2020 election.

Both the insecurity of Pennsylvania's existing paperless voting systems and the lack of auditability make replacing these machines an urgently and immediately necessary step to secure Pennsylvania's elections. Officials can and should replace Pennsylvania's paperless voting machines (DREs), which do not have voter-marked paper ballots. The Department of State has taken important steps toward this end by requiring that counties have voter-verifiable paper-record voting systems selected by the end of 2019. Pennsylvania must ensure its new voting systems meet current best practices and can be put in use without an undue financial burden on counties.

Separate from—but inextricably linked to—voting machines, multiple back-end voting-related functions are also at risk of cyberattack on their specialized election management software.[2] This is true in Pennsylvania, as it is throughout the United States, with varying levels of vulnerabilities. As a U.S. Senate Intelligence Committee interim report noted, "... potentially vulnerable systems include some of the core components of U.S. election infrastructure, including systems affiliated with...vote casting, vote tallying, and unofficial election-night reporting to the general public and the media."[3] These functions (e.g., ballot building, tallying, and reporting) are diverse and vary within Pennsylvania at the county level, both in function and in level of risk.

Security experts agree that voter-marked paper ballots (either by hand or machine) are a necessary component of secure voting machines. Ensuring that voting systems provide a paper record that the voter reviews (a "software-independent record") "provides an important security redundancy that should act as a deterrent to cyber-attacks and should provide voters with more confidence that their votes have been counted accurately."[4] The presence of paper ballots does not *prevent* errors or attacks. Indeed, similar vulnerabilities exist in systems that include voter-marked paper ballots. However, a paper record allows jurisdictions to detect any problems with the tabulation software and recover from it.

A transition to voting machines with voter-marked paper ballots (by hand or device) and implementation of cybersecurity best practices to shore up the security of election management systems (and other elements of the election architecture) should reduce the likelihood of successful cyberattacks. When coupled with robust post-election audits (described elsewhere in this report), these efforts can mitigate the consequences of attacks by ensuring detection and making it possible to recover from any attacks or errors.

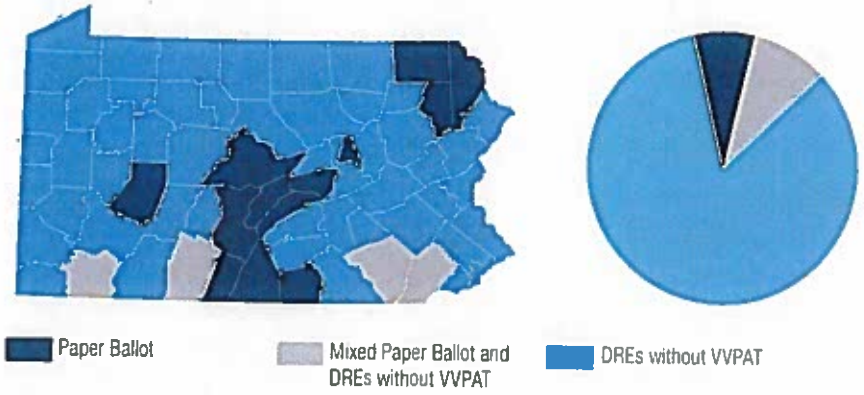
Although there is no publicly available evidence to support the conclusion that recent election results (in Pennsylvania or elsewhere) were compromised, the risk nonetheless remains, and it is imperative that officials take steps to address these vulnerabilities before the 2020 election.

PENNSYLVANIA'S VOTING SYSTEMS AND THEIR VULNERABILITIES

During the 2016 presidential and the 2018 midterm elections, more than 80 percent of Commonwealth voters were registered to vote in precincts using voting systems known as "DREs without VVPAT" (direct-recording electronic systems *without* a voter-verifiable paper audit trail).[5] Unfortunately, however, computer scientists and cybersecurity experts, as well as most election administration officials, agree that these are the country's most insecure voting systems. There is a remarkable consensus of experts regarding the insecurity of these machines.[6] The DRE systems used in Pennsylvania and elsewhere have widely known exploitable vulnerabilities.[7]

As of November 2018, only thirteen of sixty-seven counties in Pennsylvania used optical scan systems as primary polling place equipment,[8] which security experts recommend as best practice in combination with meaningful audits. These counties were Adams, Centre, Franklin, Fulton, Huntingdon, Indiana, Juniata, Lackawanna, Mifflin, Montour, Snyder, Susquehanna, and Wayne counties.

POLLING PLACE EQUIPMENT IN PENNSYLVANIA
NOVEMBER 2018



Source: Verified Voting, The Verifier—Polling Place Equipment in Pennsylvania—November 2018
www.verifiedvoting.org/verifier/#year/2018/state/42

HOW ARE PENNSYLVANIA'S DRE VOTING SYSTEMS VULNERABLE?

There have been several high-profile examples of researchers hacking voting machines like those in use in Pennsylvania. In 2007, a Princeton University computer scientist, Andrew Appel, bought a used Sequoia AVC Advantage voting machine. Appel's then-graduate student, J. Alex Halderman, was quickly able to gain access to the machine's memory and software, altering them in such a way that made modification of vote counts easy and detection difficult.[9] More than a decade later, 574 precincts in Pennsylvania in Montgomery and Northampton counties still use that model.[10] In 2017, at DEF CON's Voting Village, attendees hacked the 25 pieces of election equipment available within three days, including voting machines in use in Pennsylvania (such as the ES&S iVotronic, the AVC Edge, and the AccuVote TSx), albeit under circumstances markedly different from those in polling places.[11] During the 2018 DEF CON Voting Village, attendees again exposed weaknesses in the latter two machines.[12]

The lack of voter-marked paper ballots (either by hand or machine) retained for recounts or audits in the majority of Pennsylvania's voting machines is perhaps most potentially damaging to the legitimacy—and faith therein—of Pennsylvania's vote. If the records are corrupted, whether intentionally by malicious attack or from benign malfunction, there might be no way to know.

The lack of a paper trail prevents Pennsylvania's counties from having the usual means for detecting any hacking or error, then recovering from such an event. In the event of a suspected attack, without a paper record, counties would be unable to verify that voting records on machines were accurate. And if a county cannot credibly prove that the outcome of its vote is accurate,[13] the assertion of a successful hack could be just as damaging as a successful hack. An attack would not have to change the outcome of a vote to impact the public's faith in the reported outcome of the vote.

Nor could officials conduct an effective recount. Meaningful recounts even in the absence of a suspected attack are nearly impossible without a contemporaneous paper record of votes. Thus, Pennsylvania would be unable to undertake robust, manual recounts, which voters have come to expect in races with razor-thin margins of victory.

The U.S. Department of Homeland Security Secretary testified before the U.S. Senate Select Intelligence Committee that the inability to audit election results in states such as Pennsylvania poses a threat to national security.[14]

Testifying before Congress, University of Pennsylvania computer scientist Matt Blaze outlined the cybersecurity risks on existing DRE voting systems used in Pennsylvania and elsewhere:

> "DRE-based systems introduce several avenues for attack that are generally not present (or as security-critical) in other voting technologies. Successful exploitation of any one of these attack vectors can compromise elections in ways from which it may not be possible to recover:
>
> - Alteration or deletion of vote tallies stored in internal memory or removable media,
> - Alteration or deletion of ballot definition parameters displayed to voters,
> - Alteration or deletion of electronic log files used for post-election audits and detecting unauthorized tampering."

He went on to note that "[t]hese attacks might be carried out in any of several ways, each of which must be reliably defended against by the DRE hardware and software:

- Direct tampering with data files stored on memory cards or accessible through external interface ports,
- Unauthorized replacement of the certified software running on the machine with a maliciously altered version,
- Exploitation of a pre-existing vulnerability in the certified software."[15]

Threat Scenario

A nation-state adversary could pursue an aggressive disinformation campaign across social media, falsely claiming to the public that vulnerable machines were hacked. The adversary could point to several potential vulnerabilities.

Because Pennsylvania's paperless DRE systems do not have a paper trail, officials would be unable to conduct the kind of post-election audit or recount that could assuage the public that results should be trusted. As a result, officials might lack the necessary means to rebut the disinformation campaign.

> "Combine the patience and resourcefulness of a nation-state adversary with the unacceptably poor state of security engineering in our voting systems, and especially if we consider the possibility of insider threats, then yes, it's entirely reasonable to consider attacks against our voting systems to be within the feasible scope of our adversaries' capabilities. The best mitigations we have for systems that we use today are only feasible where we have paper ballots."
>
> Dr. Dan S. Wallach, Professor, Department of Computer Science Rice Scholar, Baker Institute for Public Policy Rice University, Houston, Texas
>
> Testimony Before the House Committee on Space, Science, and Technology hearing titled "Protecting the 2016 Elections from Cyber and Voting Machine Attacks," September 13, 2016

To summarize, there are multiple available methods of attack on Pennsylvania's most common types of voting systems—and, if well executed, attacks would not leave forensic trails behind. Many of the vulnerabilities stem from the closely connected election management systems.

PENNSYLVANIA'S ELECTION MANAGEMENT SYSTEMS AND THEIR VULNERABILITIES

Election management systems are inextricably linked to the equipment on which Pennsylvanians cast their votes. Like those voting machines, multiple back-end voting-related functions are at risk of cyberattack on their specialized election management software. Ballot building, vote tallying, and election-night reporting are among the principal back-end activities—all of which present cyber-related risks to Pennsylvania's election security.

Functions of Pennsylvania's election management systems are diverse and vary within Pennsylvania at the county level, including in terms of connectedness to the Internet. Although there are components at both state and local levels that play a key role in the broader election system architecture, counties are the key players for these critical election management systems. For example, the Department of State does not have responsibility for ballot building, nor does its election-night reporting system connect with county election management systems. County-level systems handle the primary back-end activities for which election officials are responsible, making securing these systems all the more complex.

Ballot Building and Vulnerabilities

Officials must program all electronic voting systems—including both DRE and optical scan systems—before any election. For electronic voting machines like DREs, the input is a ballot definition file and, for some machines, an activation key that must be loaded onto the machines.[16] Even for optical scan machines, officials must program the machines before voting via election preparation and ballot tabulation software.[17]

Take, for example, the ES&S iVotronic DRE machine—a common DRE machine that 26 Pennsylvania counties use.[18]

Source: ES&S
https://www.essvote.com/products/3/6/DRE/ivotronic/

Prior to voting, election officials load ballot data for each precinct via the Unity software onto a device called a Personal Electronic Ballot (PEB) to be used at the polling place. The PEB is a small, cartridge-like device ("not much larger than a pack of cigarettes, containing a battery, a microcontrollery, and non-volatile memory").[19] Once a voter's eligibility to vote has been verified, a poll worker then uses the PEB to enable that person to vote. The PEB communicates with the DRE via infrared communications, enabling the voter to proceed with voting on the DRE.[20]

Carnegie Mellon University researchers identified three potential attack scenarios targeting PEBs in Allegheny County, which uses the common ES&S iVotronic DRE: (1) attacking PEBs in the Election Division before PEBs are delivered to polling places by gaining access to the PEB writer and modifying PEBs, (2) attacking DREs via compromised PEBs in a polling place, and (3) compromising the Unity software via a malicious PEB.[21]

There are similar ballot-building software vulnerabilities in other models of paperless DREs in use in Pennsylvania, including the AccuVote TSx, which 16 Pennsylvania counties used in November 2018.[22]

Threat Scenario

An insider—such as a county election official or seasonal worker—could use his or her access to voting equipment to introduce (maliciously or inadvertently) compromised software into machines.

Such personnel often have substantial access to voting equipment, particularly on Election Day. By physically inserting a compromised PEB (or similar external media for machines that do not use a PEB) into machines, the insider could load malicious code or manipulated software onto the machines to change the tally of votes.

Without a paper trail to audit after the election, officials would have little chance of detecting the insider attack.

Tallying and Election-Night Reporting—and Vulnerabilities

The back-end functions of tallying and election-night reporting are closely connected—and both are vulnerable to cyberattack.

Tallying[23] is the aggregation of individual votes for purposes of determining totals and results. Tallying of votes in Pennsylvania can begin at the polling place, the precinct level, or even the county level. Like many election-related activities, there is much variance in practice across Pennsylvania. The level of network connectedness of the relevant components used in tallying also varies.

Election-night reporting is the publication of tallying results to the public, which involves reporting unofficial results. Election-night reporting is connected closely to the tallying function and is typically achieved through posting results on the Internet.[24] For *official* results, county officials must comply with the Election Code's requirements for the tabulation and certification of results, which counties must provide to the Department of State.[25]

In Allegheny County, for example, once a polling place is closed, poll workers close the machines and tabulate the precinct result. Allegheny County (and twenty-five others in Pennsylvania) used in November 2018 the paperless ES&S iVotronic DRE machines, which require a poll worker to close the machines with the PEB. After precinct results are printed, workers gather flash cards with summary results data from each machine, along with absentee, provisional, and emergency ballots, and then physically transport these materials from individual precincts to regional centers. Software then reads the results, which Allegheny County personnel send to the County Tabulation Center by modem landline. The software at each regional center analyzes the PEBs to obtain the official tabulation of votes, supplemented by analysis of the flash cards, if necessary.[26] After this process, election-night reporting occurs when the unofficial results are posted to a public-facing web portal.[27]

The Commonwealth also publishes unofficial results on a public-facing website, with data derived from county reporting of results.[28]

There are multiple potential points of exposure during tallying and election-night reporting.

There are multiple potential points of exposure during tallying and election-night reporting. The primary concern is an attack that could compromise the integrity or the availability of the tabulation of votes.

The vulnerabilities associated with ballot building described above, of course, relate to tallying and reporting and could lead to a compromise of vote aggregation and what is reported to the public. In particular, those vulnerabilities could allow an attacker to infiltrate DRE machines (for example, through compromised ballot definition files) and take action to manipulate the count of votes. The software that analyzes PEBs to tabulate votes in the common ES&S iVotronic DRE machines, for instance, also presents a potential vulnerability, with implications for tallying and reporting. Such an attack, undermining either the vote count or the reporting of the count to the public, could pose a threat to faith in elections and democracy.

Additional tallying-related risks stem from the transmission of tallying data to centralized locations through either removable media or even direct connections (such as phone calls, modem landlines, local network connections, and the like).[29] Attackers could expose removable media (such as flash drives, memory cartridges, and PEBs) to malware or otherwise compromise them through prior use or in the supply chain. Where data transmissions are made via network, configuration errors in network connections (e.g., modems) can expose the process to "man-in-the-middle" attack vulnerabilities.[30] Such an attack would allow the attacker to "'listen' in on transmissions, intercept data that is specifically targeted as valuable, and capture the data. Sometimes this data can be modified in the process of transmission to try to trick the end user to divulge sensitive information, such as log-in credentials."[31]

In a 2018 report on election security in the states, the Center for American Progress rated Pennsylvania's ballot accounting and reconciliation procedures as "unsatisfactory."[32] The report identified a specific tallying vulnerability: "Counties are not explicitly required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct amount."[33] Although county officials are not "explicitly required" to compare countywide results to precinct-level results on election night or during the official canvass, according to the Department of State, the official canvass is conducted in such a way that countywide results cannot be ascertained independently of precinct-level results. In order to mitigate the possibility of discrepancies in reporting between countywide totals and precinct totals, the Department of State provides counties with a reconciliation tool that displays the countywide totals reported compared to the aggregate of the precinct totals and flags any discrepancies.[34] Nonetheless, it would be useful to memorialize a county requirement to compare countywide and precinct-level results, and to account for each memory card containing votes and confirm that all votes were aggregated in the total, which the commission encourages either through the Pennsylvania Department of State's "Post-Election General Reconciliation Checklist"[35] or some other mechanism. Such a measure would give election officials and the public additional confidence that results are correct.

Election-night reporting itself also faces threats, largely stemming from the transmission of results to public-facing websites. As with tallying, "man-in-the-middle" attacks are a key threat to election-night reporting, with hackers potentially manipulating results during transmission. A potential distributed denial of service (DDoS) attack on public-facing websites is another key threat, which could cripple such websites and make election-night reporting unavailable. Website spoofing, whereby an attacker redirects the public to a spoofed website controlled by the attacker (likely part of a disinformation campaign), is yet another relevant threat.[36] In practice in Pennsylvania, most counties transmit unofficial election-night returns through the Department of

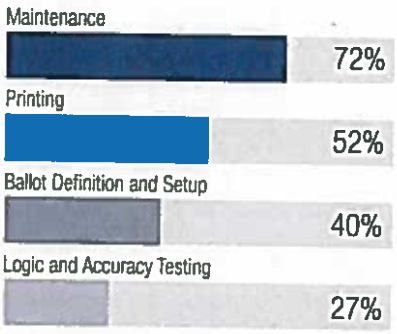
State's Election-Night Returns application. Counties must transmit those returns using a county computer that is not connected directly to any of the components of the voting system, including the computer on which the election management system resides. A smaller set of counties report unofficial election-night returns via fax, or the Department of State manually scrapes the returns from the county's website.

The possibility of compromise of vote tallying systems and the corresponding risks to election-night reporting highlight why electronic voting systems that incorporate voter-marked paper ballots that are retained for recounts and audits, as well as implementation of risk-limiting tabulation audits and audits of other key election processes, are so critical to securing elections.

Vendors and Supply Chains—and Vulnerabilities

Vendors play a major role in administering elections in Pennsylvania. According to the Joint State Government Commission's report on *Voting Technology in Pennsylvania*, more than 75 percent of Pennsylvania counties use vendors to perform some election-related work.[37] This figure, although striking, does not fully capture the reach of vendors because the figure does not take into account universal county use of vendor equipment, such as voting machines and e-pollbooks.

PERCENT OF COUNTIES USING OUTSIDE VENDORS FOR ELECTION FUNCTIONS



Data from Joint State Government Commission
Report of the Advisory Committee on Voting Technology in Pennsylvania—as of December 2017
http://jsg.legis.state.pa.us/publications.cfm?JSPU_PUBLN_ID=463

Vendor involvement in facets of county election management systems provides adversaries with an appealing attack vector. In fact, the Special Counsel's indictment of Russian operatives included allegations that they hacked a U.S. election vendor.[38]

As an illustrative example, attackers could target vendors that provide ballot definition and setup services to counties. In such an attack, if a nefarious attacker were to gain access to the original ballot definition file, voting machines could be susceptible to a wide range of attacks that could disrupt voting, alter outcomes, and more.[39] The attacker could accomplish this by gaining access to vendor systems—something that, according to Professor J. Alex Halderman's presentation to the commission, an attacker could accomplish through a spear-phishing campaign. Such a campaign could entail mining data about vendor personnel and email addresses from vendor websites, then using that data to craft spear-phishing emails that would allow an attacker to gain system access if recipients were to open an attachment or click an embedded link, for

Threat Scenario

Using publicly available information about which vendors provide election services in Pennsylvania counties, hackers could mine LinkedIn, vendor websites, and other public resources for information about vendor employees and their email addresses. Using that information, hackers could then send spear-phishing emails to vendor employees.

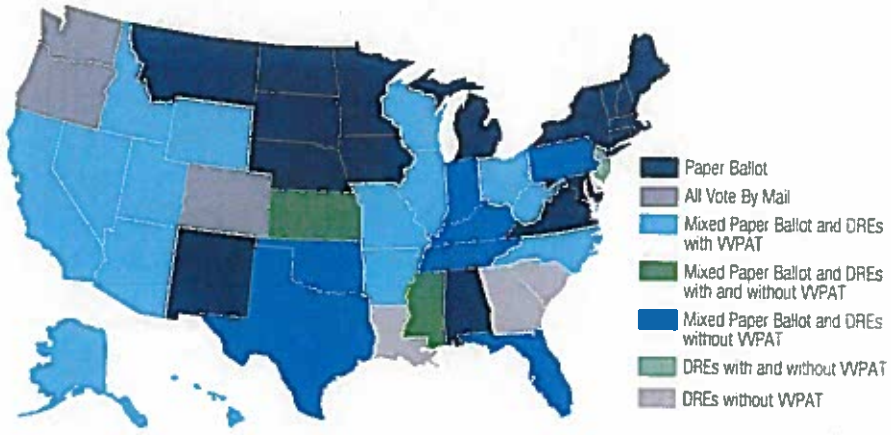
Once the hackers gained access to vendor systems through a successful spear-phishing attack, the hackers could use that infiltration to manipulate the software that a vendor would install on county voting machines in connection with ballot programming. Such compromised software could enable the hackers to alter the vote count, with little chance of detection given the lack of a paper trail.

instance. With access, an attacker could install malicious code on that software, which the vendor would eventually install on voting machines when providing ballot definition and setup services.

Vendor supply chains present another potential vulnerability. Whether sourcing parts and equipment from downstream vendors or manufacturing materials in-house, vendor supply chains are often quite opaque to election officials. And, given the fiscal reality of county election offices, election officials simply lack the means to meaningfully inspect or assess vendor supply chains. Consequently, supply chains can be a significant weakness in vendor cybersecurity, particularly where vendors source parts or materials from abroad.

PENNSYLVANIA'S USE OF DRE MACHINES MAKES IT A NATIONAL OUTLIER

Nationwide use of DRE machines has declined significantly since 2006. In 2016, nearly half of U.S. registered voters lived in jurisdictions that used optical scan systems as their primary voting systems, and more lived in jurisdictions using both optical scan and other systems, according to The Pew Research Center, analyzing Verified Voting data.[40] Only Delaware, Louisiana, Georgia, New Jersey, and South Carolina still use only DRE systems statewide as their primary voting systems (and Delaware and Louisiana are in the process of replacing those machines). Pennsylvania is one of nine states that use a combination of paper ballots and electronic machines without a paper trail.[41]



Source: Verified Voting, The Verifier—Polling Place Equipment—November 2018 https://www.verifiedvoting.org/verifier/

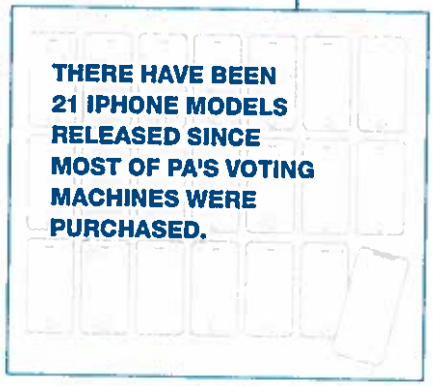
Several states, including California, Ohio, New Mexico, and Virginia, have decertified voting machines that are still in use in multiple counties in Pennsylvania. As just one example, as of November 2016, more than 54 percent of Pennsylvania voters were voting on systems (as their primary voting method) decertified in Virginia for security reasons.

VOTING SYSTEMS DECERTIFIED IN VIRGINIA BUT STILL USED IN PENNSYLVANIA

Vendor	Number of Pennsylvania Counties	Registered Voters as of November 2016	Percentage of Registered Voters
Premier/Diebold	16	894,938	10.63%
Sequoia AVC Advantage	2	755,196	8.97%
Sequoia Edge	1	297,886	3.54%
Hart eSlate	1	75,193	0.89%
ES&S iVotronic	24	2,588,325	30.74%
TOTAL	**44**	**4,611,538**	**54.77%**

Source: Verified Voting, https://www.verifiedvoting.org/verifier/ Data accessed June 12, 2018

PENNSYLVANIA'S VOTING SYSTEMS ARE INSECURE AND NEARING THE END OF THEIR LIFE CYCLES



Data from Brennan Center for Justice America's Voting Machines at Risk—2015 https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf

The significant majority of voting systems used in the state today were purchased more than a decade ago.[42] Not only were these systems not designed to withstand hacking, most are nearing the end of their usable lives. In fact, according to the Brennan Center for Justice, in 2018, 41 states were "using systems that are at least a decade old, and officials in 33 say they must replace their machines by 2020."[43] With aging machines, "essential parts like memory cards and touch screens fail," and these older "machines are more likely to use outdated software like Windows 2000," posing "serious security risks."[44] Some officials have even resorted to eBay to buy replacement parts for these old machines.[45] The Presidential Commission on Election Administration called this state of affairs an "impending crisis in voting technology."[46]

Unsurprisingly, paperless DRE machine issues caused substantial delays and disruptions to election administration during the 2018 midterm elections, including failure of machines in Georgia, broken machines in several Philadelphia precincts, calibration problems elsewhere in Pennsylvania and in South Carolina, and vote-flipping issues in Texas.[47] In other words, even without security flaws, most Pennsylvania counties would likely replace their voting systems within the next few years due to age.

WHAT VOTING SYSTEMS SHOULD PENNSYLVANIA USE?

Recommendation 1: Replace Vulnerable Voting Machines with Systems Using Voter-Marked Paper Ballots.

Counties using DREs should replace them with systems using voter-marked paper ballots (either by hand or by machine) before 2020 and preferably for the November 2019 election, as directed by the Pennsylvania Department of State.

The Department of State should decertify DRE voting systems following December 31, 2019, if not sooner.

Security experts widely consider best practice for voting systems to be paper ballots either filled out by voters or marked with a ballot-marking device and then tabulated by

optical scanners.[48] Optical scan systems provide the assurance of auditability and, if necessary, the means to conduct a recount.[49]

Illustrating this consensus view, a recent report on election security from the National Academies of Sciences, Engineering, and Medicine observed that "[e]lectronic voting systems that do not produce a human-readable paper ballot of record raise security and verifiability concerns." The report recommended that paper ballots "be marked by hand or by machine (using a ballot-marking device) ... [and] counted by hand or by machine (using an optical scanner)."[50] Similarly, Rice University Professor Dan Wallach testified before Congress that although "[o]ptical scan systems face all the same electronic tampering threats from adversaries, ... these threats can be mitigated by robust paper auditing procedures."[51]

Ensuring that voting systems provide a paper record that the voter reviews (a "software-independent record") "provides an important security redundancy that should act as a deterrent to cyberattacks and should provide voters with more confidence that their votes have been counted accurately."[52] The presence of paper ballots does not *prevent* errors or attacks. Indeed, similar vulnerabilities exist in systems that include voter-marked paper ballots. However, paper records allow jurisdictions to detect any problems with tabulation software and recover.

In other words, a determined adversary can almost certainly hack any technology. But optical scan systems provide the assurance of auditability and, if necessary, the means to conduct a full recount.[53] As the Advisory Committee on Voting Technology to the Joint State Government Commission found, "the national conversation surrounding elections, especially regarding the possibility of voting machine hacking, has made it clear to the Advisory Committee members that implementing technology that reduces the possibility of hacking, and that facilitates post-election audits and recounts, is the best means of maintaining voter confidence."[54]

Pennsylvania therefore took a significant step forward in improving its election security when the Department of State directed on April 12, 2018, that all Pennsylvania counties have "voter-verifiable paper-record voting systems selected no later than December 31, 2019, and preferably in place by the November 2019 general election."[55] Per an earlier directive, any election systems purchased from February 9, 2018, onward must include a paper audit capacity.[56] More recently, in settling federal litigation stemming from presidential candidate Jill Stein's lawsuit challenging Pennsylvania's recount procedures and use of DRE voting systems, among other things, the Department of State agreed to "continue to direct each county in Pennsylvania to implement [paper-based] voting systems by the 2020 primaries, so that every Pennsylvania voter in 2020 uses a voter-verifiable paper ballot."[57] This settlement reinforces the earlier directives and adds the backstop of a federal court with jurisdiction to enforce the settlement agreement if need be.

The Department of State should not certify and counties should not procure DRE machines—not even with voter-verifiable paper audit trails—but instead systems that tabulate voter-marked paper ballots, which are retained for recounts and audits.

Optical Scan Systems: How Do They Work?

"[O]nce the voter is authenticated and checked in, the voter is given a paper ballot. (The ballot is similar to the absentee ballot you would receive in the mail if you needed to vote absentee.) The ballot lists the candidates and ballot questions, and beside each one is a small circle or bubble. The voter is given a ballot and a "privacy sleeve" (this is essentially a folder to protect ballot secrecy after the ballot is marked). The voter takes the ballot to a table or desk that affords a private place to mark the ballot and the voter then marks his/her choices by filling in the bubbles with a pen. The voter brings the ballot, in the privacy sleeve, to an optical scanner which is fitted on top of a secure ballot box. The voter feeds the ballot into the scanner. If the voter over-voted, the scanner will reject the ballot and return it to the voter so a poll-worker can spoil the ballot and the voter can correct the over-vote on a new ballot. The scanner can also be set to alert voters if they under-vote. After the ballot is accepted by the scanner, the ballot drops into the secure ballot box."

Commission Member Marian Schneider, testimony to the Pennsylvania Senate State Government Committee, December 12, 2017

Threat Scenario

Sophisticated hackers could exploit wireless communications between e-pollbooks in polling places. A common function of e-pollbooks, wireless connectivity provides an opening for hackers to gain access to connected devices and components. Once hackers succeed in infiltrating through a network, they might manipulate devices to disrupt voting through a range of actions:

- Disrupt e-pollbook connectivity
- Shut down or freeze e-pollbooks
- Maliciously delete or alter registration records
- Change whether individuals have already voted on Election Day or via absentee ballot

This type of attack could frustrate voters, expose polling places to fraud, and undermine effective election administration.

The Commonwealth should *not* certify new DRE electronic voting systems, regardless of whether the system includes voter-verifiable paper audit trails. If the Commonwealth were to certify such machines, Pennsylvania counties should not procure those machines given the security weaknesses of DREs relative to optical scan systems. Voters rarely inspect the paper records printed by voting machines, the printers can have technical difficulties, and the paper can be fragile and difficult to audit.[59]

Concerns about Purchasing New Voting Systems

Accessibility Concerns with Optical Scan Machines

Optical scan systems offer Help America Vote Act of 2002 (HAVA) compliance[59] through use of a ballot-marking device, allowing voters who have a disability that would make it difficult to hand-mark a ballot the ability to do so privately and independently. The commission notes with concern, however, that not all ballot-marking devices are as accessible as some DRE machines for voters with some disabilities.[60] Although most ballot-marking devices allow voters to *mark* their ballots privately and independently, they sometimes do not allow for voters to then *verify* and *cast* their votes privately and independently, depending on the voter's disability.[61] Moreover, even where ballot-marking devices do allow for such private and independent voting, officials must be cognizant of accessibility issues within and around the polling place.[62] The commission also notes that ballot-marking devices have their own security concerns—for example, some ballot-marking devices have the capability to print on the ballot after the voter's last chance to verify, which exposes the ballot to unverifiable change—highlighting the importance of instituting statistically sound audits of paper ballots.

Pennsylvania's goal should be for all voters to be able to vote independently, privately, and securely. This means that all voters should be able to mark, verify, and cast their votes with privacy and independence—and with confidence in the security of their votes.

The Department of State should therefore demand more accessible solutions for ballot-marking devices and to prevent the adoption of ballot-marking devices with inappropriate printing abilities. Counties might consider leasing or other limited purchasing options for the immediate future and look to set aside future funds to procure ballot-marking devices as better accessibility technology becomes available.

Feasibility of Changeover to New Voting Systems

Changing from paperless DRE machines to voting systems involving voter-marked paper ballots is feasible throughout Pennsylvania before the 2020 election, as evidenced by other states' experiences. Virginia overhauled its paperless DRE voting machines and switched to a statewide voting system of paper ballots combined with optical scanners just weeks before the 2017 elections. This involved changing systems used by roughly 190,000 of the state's 5 million registered voters,[63] although Virginia jurisdictions had far less notice than Pennsylvania counties have now and received no state funding support. Delaware and Louisiana, for example, are also in the process of replacing their current DRE voting systems that lack paper records, with a target of completion by 2020.[64]

Pennsylvania requires that any voting systems procured by counties must achieve certification from both the U.S. Election Assistance Commission and the Secretary of the Commonwealth.[65] As of January 4, 2019, the Department of State has certified since January 1, 2018, only three newer systems for use in Pennsylvania: (1) the Unisyn Voting Solutions OpenElect 1.3.0.2.A Voting System, (2) the ES&S EVS 6.0.2.1 Voting System, and (3) the Unisyn Voting Solutions OpenElect 2.0A2 Voting System.[66] Officials expect to certify additional systems in the near term, for a total of six expected systems.[67] While recognizing that much of the speed with which the state is able to certify voting systems is dependent on vendors, the commission advises the state to move as quickly as possible so as to provide counties with ample time for procurement and training.

The commission recognizes that deployment of new systems is no simple task. It requires training of county election personnel, poll workers, and even voters. Therefore, the commission urges counties to move as quickly as possible to have new systems in place for the November 2019 election (if not sooner) so that the first use of new voting systems is not during the 2020 election, when many more voters are anticipated.

HOW SHOULD PENNSYLVANIA PAY FOR NEW VOTING SYSTEMS?

Recommendation 2: The Pennsylvania General Assembly and the Federal Government Should Help Counties Purchase Secure Voting Systems.

Pennsylvanians, including public officials, must recognize that election security infrastructure requires regular investments and upgrades. Our elections—and Pennsylvanians' faith in them—are not free.

The General Assembly should appropriate funding to help cover the cost of counties' purchase of voting systems that incorporate voter-marked paper ballots (marked either by hand or by ballot-marking device) and other needed improvements to Pennsylvania's election security.

The cost of procuring new voting machine systems is not trivial for counties. The Department of State estimated the cost of new voting machines to replace paperless DREs to be $95 million to $153 million statewide.[68] The County Commissioners Association of Pennsylvania estimated the cost at $125 million[69]—or $9.76 per Pennsylvanian. However, compared to the magnitude of the risk posed by insecure voting machines, the cost is a relative bargain.

WE COULD REPLACE OUR OUTDATED VOTING MACHINES FOR THE COST OF A PITTSBURGH SANDWICH TOPPED WITH FRIES AND SLAW OR A PHILLY CHEESESTEAK FOR EVERY PENNSYLVANIAN

The commission urges the Governor to include significant funding for voting machine replacement in the upcoming budget. Likewise, the commission urges the General Assembly to appropriate this funding.

DRE machines, with or without voter-verifiable paper audit trails, are typically more expensive than optical scanners because precincts using DRE machines typically require one machine per 250–300 voters[70] and have higher maintenance costs than optical scanners.[71] Optical scanners, including the associated ballot-marking device for HAVA accessibility, are estimated to cost about $6,200–$10,000 per precinct.[72] For many counties in Pennsylvania, replacing existing DRE machines with optical scan systems will likely be less expensive than replacing them with newer DRE machines or using ballot-marking devices for all voters.[73]

The U.S. Congress should provide additional appropriations for states, like Pennsylvania, which need to replace significant numbers of DREs without voter-verifiable paper audit trails.

Pennsylvanians should support federal legislation that includes assistance for states to replace aging voting systems.

The federal government has offered some funding help, but not nearly enough. Congress allocated to Pennsylvania only $13.5 million in last year's election security grants.[74] The Commonwealth's required matching funds bring this amount to $14.2 million, leaving a substantial funding gap. Although the commission hopes (and strongly urges) that additional federal funding will be forthcoming, the Commonwealth and its counties should not rely on congressional action.

The Governor, General Assembly, and counties should explore creative financing mechanisms (such as a bond issuance) to assist counties with procuring more secure electronic voting systems with voter-marked paper records.

It is possible to upgrade voting systems without outright purchasing. Possibilities include leases and combinations of low-interest loans or grants. Pennsylvania officials have said publicly that they are exploring these options.[75] Other creative financing ideas that states have explored may be available as well.[76]

Pennsylvania officials should also consider the feasibility of a bond issuance as a potential funding source for the purchase of new voting equipment. Under the Pennsylvania constitution, bonds may be used as a funding source for capital projects; public referendums are not required for such bonds.[77] Because a statutory definition of "capital project" includes "infrastructure" as well as "furnishings, machinery, apparatus or equipment for a building, structure, facility or physical public betterment or improvement,"[78] the purchase of voting equipment should constitute a capital project. Consequently, the commission urges Pennsylvania officials to explore this funding avenue, as well as consider whether there might be some arrangement whereby counties can engage in cost-sharing with the Commonwealth for service of the debt.

The General Assembly should also consider creating a fund for regular future appropriations as upgrades in security and accessibility technologies merit.

A 10- to 15-year cycle of replacing voting systems appears to be the new normal. Therefore, the commission urges the General Assembly and the executive branch to work together to create a new, permanent election security fund, which would accrue money annually for the future replacement of equipment. This approach could spread the costs of machine replacement over several years and lessen the fiscal impact.

HOW SHOULD PENNSYLVANIA REMEDY CYBER RISKS TO ITS ELECTION MANAGEMENT SYSTEMS?

Like any cyber defensive effort, it impossible to eliminate every possible vulnerability in Pennsylvania's varied election management systems. But the suggestions that follow—cybersecurity best practices, awareness training, and assessments—can help to *improve* cyber defense and thus mitigate some of the vulnerabilities and weaknesses in these critical systems.

Recommendation 3: Implement Cybersecurity Best Practices throughout Pennsylvania's Election Architecture.

Review and, where not already in place, implement cybersecurity best practices across Pennsylvania's election architecture.

Pennsylvania officials should institute basic cybersecurity best practices, where they have not been instituted already. Several of these best practices are reflected in existing Department of State guidance.[79]

At a basic level, officials should consider for immediate implementation several best practice improvements, including patching software, using strong passwords, adding multifactor authentication wherever feasible, and adding access controls. The commission identified a few specific recommendations from among the myriad best practices that ought to define Pennsylvania's election architecture.

The Center for Internet Security's *A Handbook for Elections Infrastructure Security* provides an excellent list of best practices for potential implementation throughout the election architecture. The commission urges officials to consult this resource.[80] These and other relevant best practices should already be in place (and often are) throughout Pennsylvania. Where they are not, the commission recommends support for immediate adoption.

The commission offers several specific practices to consider for implementation (where not already in place) but stresses that this is not an exhaustive list:

- Require any entity, including county governments, that connect to the Commonwealth's networks to adhere to the Commonwealth's information technology policies, especially relating to network security.
- Ensure that algorithm choices as well as key management and risk frameworks conform to recommended federal information security standards published by the National Institute of Standards and Technology.
- Ensure that all data files use open, documented data formats.
- Require that Pennsylvania retain ownership of intellectual property it has funded.
- Any custom software should be made as a work for hire, with no rights retained by contractors or subcontractors, with all source code, build tools, and environment delivered to Pennsylvania to use as it sees fit.
- Third-party proprietary software packages may be delivered under a contractor's license only if those packages and licenses are pre-approved by Pennsylvania.
- Proprietary software packages that are proprietary to contractors or subcontractors may be delivered only if disclosed in advance in the proposal.

In addition, there are no-cost, private-sector resources that may be of use to election officials in Pennsylvania. For example, Google's Project Shield[81] and Cloudflare's Athenian Project[82]—both free services—can, among other things, defend public-facing websites from DDoS attacks.

Ensure vote-tallying systems: (1) are single-use systems; (2) are air-gapped; and (3) follow the one-way, one-use removable media rule. Have redundancies in reporting tallies.

Vote-tallying systems should: (1) be *single-use systems*; (2) be *air-gapped* (i.e., isolated from any networks or overall Internet connectivity); and (3) follow the *one-way, one-use* removable media rule. Reporting of tallies should be redundant, with tallying

submissions confirmed via phone or other secure communication. In confirming tallies, predetermined protocols should be in place to verify authorized personnel's identities. Counties should implement procedures to ensure that all memory devices are reconciled and all votes have been aggregated from each memory device into the vote totals.

Require counties to compare and reconcile precinct totals with countywide results to ensure that vote totals add up correctly.

There is no explicit requirement—either in the Pennsylvania Department of State's "Post-Election General Reconciliation Checklist"[83] or otherwise—that counties compare precinct totals with countywide results to ensure that results add up correctly. The commission suggests amendment of the checklist or some other formal means to require counties to conduct a reconciliation of precinct totals with countywide results. This requirement could instill greater confidence among the public that election results are correct.

The State and counties should be conscious of supply chain vulnerabilities. Any contractors or vendors should be assessed for security risks. Security considerations should be a key selection factor—not reviewed after a procurement decision has been reached.

The commission offers specific recommendations in the Voter Registration section regarding resources and methods to guide vendor selection and management, specifically in connection with the upcoming procurement of a new voter registration system. Nonetheless, given the central role played by vendors in election management systems, it is imperative that officials heed cybersecurity best practices to ensure that vendors are not introducing vulnerabilities into Pennsylvania's election architecture.

For example, officials should pursue open-source software where feasible or, if not, ensure that state and county offices retain ownership and/or access to any relevant software code. This will facilitate more robust and effective risk assessment and vulnerability testing of software periodically through the lifecycle of the system. The General Assembly should consider legislation to require voting system vendors to notify the Department of State and relevant local officials of any defect, fault, failure, cyberattack, or other incident affecting the hardware, software, or firmware of the voting system.[84] The commission also urges officials to require, among other things, that vendors submit to regular penetration testing, face a mandate to keep software current through updates and security patches, provide insight into supply chains, and support third-party audits.

Recommendation 4: Provide Cybersecurity Awareness Training for State and Local Election Officials.

The Commonwealth should continue to conduct cybersecurity training for state personnel. In addition, the Department of State should continue to work toward rolling out, in consultation with counties, cybersecurity training for local election officials throughout Pennsylvania.

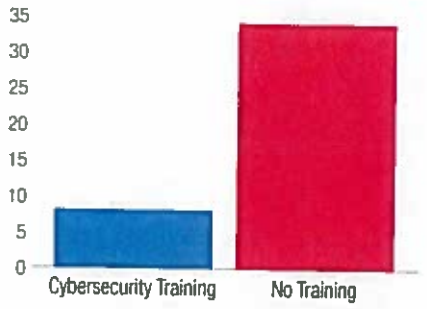
Local officials should support Commonwealth efforts to roll out cybersecurity training and creatively look to leverage existing resources to ensure personnel are adequately prepared to face today's cybersecurity threats.

Sophisticated attacks target election officials and outside election vendors with phishing schemes.[85] If such schemes are successful in compromising election officials' credentials, hackers can then use that information to penetrate sensitive election systems. In 2016, Russian military intelligence sent phishing emails to at least 122 local officials, according to an intelligence assessment.[86] And, according to the

Justice Department's indictment of Russian hackers, attackers sent more than 100 spear-phishing emails to "organizations and personnel involved in administering elections in numerous Florida counties."[87] The Russians charged also allegedly surveyed the websites of counties in Georgia, Iowa, and Florida for vulnerabilities.[88]

These targeted attacks demonstrate the importance of cybersecurity awareness at the county and state levels. Yet the Commonwealth has not been providing mandatory cybersecurity awareness training to local officials. In August 2017, election officials in Philadelphia, Allegheny, and Bucks counties told NBC News they had not received cybersecurity training,[89] and officials in those counties confirmed with the commission that they had yet to receive training from the Commonwealth as of August 2018.[90] Of the 42 counties in Pennsylvania that responded to the NBC News survey, only eight counties said that their workers had received cybersecurity training.[91] Some states, including Maryland, Virginia, and Washington, require and provide cybersecurity awareness training for local election officials.[92]

AS OF AUGUST 2017, OF THE 42 COUNTIES THAT RESPONDED TO A SURVEY, ONLY 8 COUNTIES SAID THEIR WORKERS HAD CYBERSECURITY TRAINING



Data from NBC News. Many County Election Officials Still Lack Cybersecurity Training—August 23, 2017
https://www.nbcnews.com/politics/national-security/voting-prep-e780256

The Pennsylvania Department of State reports, however, that it is committed to providing the Commonwealth's statewide cybersecurity training module to county officials.[93] As envisioned by the Department of State, training would be a mandatory condition of maintaining user credentials for the Statewide Uniform Registry of Electors (SURE)—something that should be effective in capturing the right officials across Pennsylvania. The commission commends the Department of State's efforts in this regard and encourages the rollout of this mandatory training to local election officials. The Department of State should incorporate election-specific elements (including the cybersecurity best practices referenced in this report) into the training or otherwise provide specialized training for key local personnel with election cybersecurity responsibilities. The County Commissioners Association of Pennsylvania should also continue its efforts, in partnership with the Commonwealth and Cofense (formerly PhishMe), to provide simulated phishing training to counties.

The Department of State should encourage local election officials to take advantage of federal cybersecurity training resources, such as the Department of Homeland Security's free, online, on-demand cybersecurity training system for governmental personnel and the inter-agency National Institute for Cybersecurity Careers and Studies.

Election officials should also avail themselves of federal government resources, including the Department of Homeland Security's free, online, on-demand cybersecurity training system for governmental personnel[94] and the National Institute for Cybersecurity Careers and Studies, which the department developed jointly with other governmental agencies and is an online resource for cybersecurity training connecting government officials with training providers.[95]

Recommendation 5: Conduct Cybersecurity Assessments at the State and County Levels.

The Pennsylvania Department of State should continue to conduct, and all of Pennsylvania's counties should conduct, comprehensive cybersecurity assessments. Election officials should also conduct regular process audits across the election ecosystem.

Local officials should not only support but also work closely with Commonwealth officials in connection with cybersecurity assessments.

In addition to following best practices and improving training for election officials and poll workers, state and local officials should conduct regular cybersecurity assessments. Comprehensive threat assessments and security audits should be a key element of Pennsylvania's broader election security plan.

Efforts should include penetration testing and realistic tabletop exercises to practice contingency plans for all phases of election, tabulation, audit, and recount—ensuring that Pennsylvania can recover in the face of an attack. Officials should ensure that current disaster recovery exercises involving the SURE voter registration system include tabletop exercises for recovery from attacks on election management systems and precinct-based voting systems.[96]

Election officials should avail themselves of the no-cost cybersecurity assessment resources offered by the U.S. Department of Homeland Security.

Pennsylvanians should support federal legislation that strengthens and supports federal cybersecurity resources and provides training and assessment assistance to state and local election officials.

The commission commends the Department of State for having taken advantage of the U.S. Department of Homeland Security Risk and Vulnerability Assessment prior to the 2016 and 2018 elections.

Unfortunately, DHS's Risk and Vulnerability Assessment is not focused on individual counties, which should undergo periodic assessments as well. To that end, the commission recommends that all Pennsylvania counties avail themselves of DHS's regular cyber-hygiene scans—something that the Department of State also encourages counties to do. Congress should also consider legislation to provide additional cybersecurity resources to state and local election officials.

The General Assembly should provide funding support for counties to implement regular, periodic cybersecurity assessments and audits, especially relating to election infrastructure.

More broadly, it is imperative that counties implement regular, periodic cybersecurity assessments. The cost of such assessments would vary dramatically based on scope, county size, and the like—but the Department of State roughly estimated that a risk and vulnerability assessment for one county might cost somewhere in the range of $50,000–$100,000 on the high end. Counties should also consider the Center for

Internet Security's network monitoring solution ("Albert"), which provides network security alerts to help counties identify malicious activity.[97]

As a frame of reference for what county-focused assessments and related security efforts might cost Pennsylvania, New York announced it was earmarking $5 million in fiscal year 2019 to provide counties with: (1) cybersecurity risk assessments, (2) enhanced intrusion-detection services, and (3) managed security services.[98] Where appropriate and available, the Office of Administration–Office of Information Technology (OA-OIT) should make resources available to counties for cybersecurity assessments.

Lastly, state and local election officials should incorporate regular audits of key aspects of election processes into a broader assessment strategy. Such audits should include examination of ballot preparation and dissemination, pollbook preparation and operations, chain of custody of paper ballots of voting equipment, reconciliation of vote totals, and return of election materials.

Pennsylvania's aging and insecure voting equipment represents a clear and present danger to the security of the vote.

Pennsylvania's aging and insecure voting equipment represents a clear and present danger to the security of the vote. It is paramount that officials take swift action to replace these vulnerable machines with those that incorporate voter-marked paper ballots (either by hand or by machine). Pennsylvania officials must also shore up the cybersecurity of election management systems, which are inextricably linked to the voting equipment on which voters cast their ballots.

Voter Registration System

Overview

The U.S. Senate Intelligence Committee's investigation into Russian targeting of election infrastructure during the 2016 election found that cyber actors targeted state election systems and, in some instances, successfully penetrated voter registration databases.[99] At least 18 states—and perhaps as many as 21—"had election systems targeted by Russian-affiliated cyber actors."[100] That targeting included "vulnerability scanning directed at ... Department of State websites or voter registration infrastructure."[101]

According to the Department of Homeland Security, the Russians targeted Pennsylvania's voter registration system.[102] However, per Commonwealth officials, "neither it nor the U.S. Department of Homeland Security has any evidence of a breach."[103] The system—known as the Statewide Uniform Registry of Electors (SURE)—was probed, but there is no publicly available evidence suggesting that the system was penetrated.

Officials *detected* malicious access attempts in at least six states (not including Pennsylvania), and some states even experienced intrusions that would have allowed cyber actors to "alter or delete voter registration data."[104] Of course, there may have been other attempts (including in Pennsylvania, perhaps) that remain undetected. Moreover, the Justice Department's July 2018 indictment of Russian hackers alleged that the Russians successfully hacked a state election website and stole sensitive information about half a million voters.[105] The Russian hackers also allegedly hacked the computers of a vendor "that supplied software used to verify voter registration information for the 2016 U.S. elections."[106]

If careful and proper cyber-hygiene practices are observed, the risk of alterations to the voter registration system is low because voters will likely learn of changes to records—at the latest when they attempt to vote (but hopefully before Election Day).

However, even attacks that fail to alter the ultimate results of elections could nonetheless succeed in damaging public trust in outcomes, as well as disrupt administration of elections. Either could undermine faith in democracy in Pennsylvania.

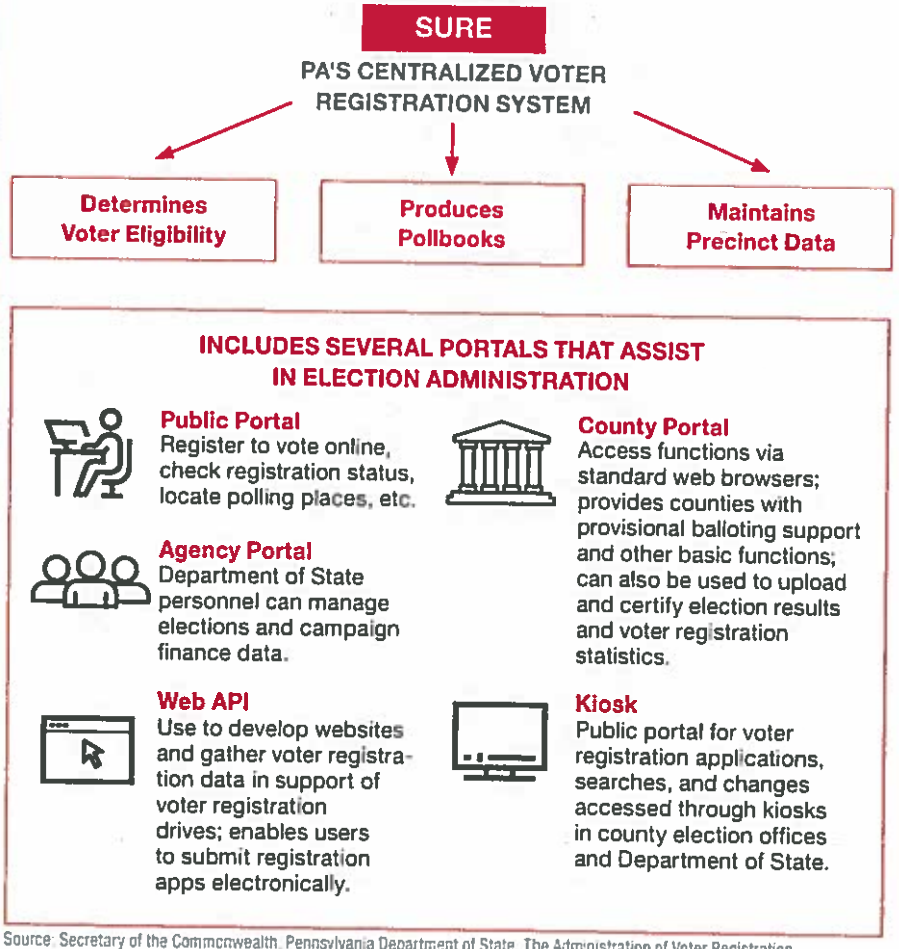
PENNSYLVANIA'S VOTER REGISTRATION SYSTEM AND ITS VULNERABILITIES

System Overview

Under Pennsylvania law, the Secretary of the Commonwealth (who heads the Department of State, including the Bureau of Commissions, Elections, and Legislation) is responsible for coordinating voter registration procedures and the SURE system.[107]

Pennsylvania's registration system is a "top-down system"—that is, one in which "data are hosted on a single, central platform of hardware and maintained by the state."[108] As described in the Pennsylvania Department of State's 2016 Report to the General Assembly:

"SURE is the centralized voter registration and election management system designed to assure the accuracy and integrity of the Commonwealth's voter registration records maintained by the election authorities in Pennsylvania's 67 counties. The SURE system is a platform that supports the critical functions of the Commonwealth's elections—from determining voter eligibility to maintaining precinct data to producing pollbooks. A centralized, uniform registry that is accessible to all county offices greatly enhances the overall accuracy and integrity of the voter registration rolls and the resulting quality of voter services."[109]



Source: Secretary of the Commonwealth, Pennsylvania Department of State, The Administration of Voter Registration in Pennsylvania: 2016 Report to the General Assembly, June 2017, at 14, http://www.dos.pa.gov/VotingElections/OtherServicesEvents/Documents/2016%20Annual%20Report%2006302017_final.pdf

The **SURE Voter Registration** application is available to counties to support a number of election-related tasks.

Since 1995, Pennsylvania has operated a paperless registration system at Department of Transportation (PennDOT) locations, and by 2005 all Pennsylvania counties had fully automated the system by accepting registration data through SURE.[110] The SURE Voter Registration application is available to counties in support of a variety of election-related functions, "including the management of vote history, absentee ballots, pollbooks, election-related reports, and voter registration correspondence to voters."[111]

There are several ways for a Pennsylvania voter to apply for registration.[112] An eligible voter can complete a voter registration form and either deliver it or mail it to their county voter registration office.[113] In-person registration is also available at county and other governmental offices (such as PennDOT locations).[114] Eligible voters can also use Pennsylvania's online voter registration application that is accessible via the Internet and is mobile adaptive.[115] Whatever the method of applying, those deemed eligible to register are ultimately entered into SURE. Thus, SURE plays the central role in Pennsylvania's voter registration system.

Threat Scenario

Sophisticated hackers could exploit wireless communications between e-pollbooks in polling places. A common function of e-pollbooks, wireless connectivity provides an opening for hackers to gain access to connected devices and components. Once hackers succeed in infiltrating through a network, they might manipulate devices to disrupt voting through a range of actions:

- Disrupt e-pollbook connectivity
- Shut down or freeze e-pollbooks
- Maliciously delete or alter registration records
- Change whether individuals have already voted on Election Day or via absentee ballot

This type of attack could frustrate voters, expose polling places to fraud, and undermine effective election administration.

In Pennsylvania, SURE also plays an important role in the generation of pollbooks by counties.

Pollbooks provide election officials with voter registration information at polling locations and "are necessary to ensure voters are registered and are appearing at the correct polling place."[116] Accurate pollbooks also play a role in managing wait times at polling places.

Local election officials in Pennsylvania are required to use data from SURE to create pollbooks.[117] A critical element of voting on Election Day, pollbooks in Pennsylvania consist, in essence, of two components: (1) the voter certificates (to be signed by individual voters during check-in at the polling place) and (2) the district register (each registrant's registration information and signature, which is compared to the signature on the voter certificate).[118] Voter certificates are included in the district register, or pollbook, so voters sign one document upon check-in.

Many Pennsylvania counties use paper pollbooks that are printed via SURE.[119] Some counties use electronic pollbooks (e-pollbooks).[120] Several e-pollbook systems are certified for use in Pennsylvania.[121] E-pollbooks are typically tablets or laptop computers that allow poll workers to look up voters in lieu of having to check paper lists. Typically, e-pollbooks are equipped with technology that enables them to communicate with a sister unit in the polling location—either over a wired connection or via a wireless network. A wireless connection, in particular, presents unique security challenges, stemming from the ability of attackers to target connections and associated devices from afar.

Regardless of whether counties use paper or e-pollbooks, the integrity and reliability of SURE are key to ensuring accurate pollbooks in polling places on Election Day.

VULNERABILITIES

As of June 2017, 41 states (including Pennsylvania) were still using voter registration databases that were initially created a decade ago or longer.[122] As the Brennan Center for Justice has observed, "[t]hese outdated systems were not designed to withstand current cybersecurity threats."[123] To be sure, age alone is not dispositive of a system's cybersecurity readiness. Yet the SURE database is into its second decade of service, although Pennsylvania officials have regularly maintained and updated its operating system.

Fortunately, Pennsylvania is poised to embark upon the process to replace the existing voter registration system (SURE) in the next three years or so[121]—an excellent opportunity to deploy best practices in selecting, developing, and implementing a registration system designed to guard against a range of cybersecurity threats while maximizing voter engagement. The Auditor General's recently announced audit of the voter registration and voting systems[125] should also provide findings that could be leveraged to inform the SURE procurement process.

In the meantime, however, SURE has vulnerabilities and faces threats that must be addressed. The commission notes that although these risks are serious, the risks associated with Pennsylvania's DRE machines present a more clear and present danger to the security of the vote.

Two specific threats to SURE are illustrative of these risks to the voter rolls: (1) alterations, deletions, or creations of registrations; and (2) DDoS attacks.

Alterations, Deletions, or Creations of Registrations

Researchers have highlighted one potential mode of attack on the voter registration system that would allow attackers to wreak havoc on registration records.

Carnegie Mellon University researchers analyzed potential vulnerabilities in Pennsylvania's entire election ecosystem—with a particular focus on Allegheny County—and identified specific attack scenarios targeting Pennsylvania's voter registration system with potential statewide ramifications.[126]

The Carnegie Mellon University report identified a "major vulnerability" based on SURE's "weak authentication required of applicants sending in registrations forms"—who are asked to provide name, current address, and a Pennsylvania driver's license or identification card number (if they have one) or, if not, the last four digits of a Social Security number.[127] The vulnerability stems from the availability of driver's license and Social Security numbers "on sites like Pastebin or for purchase on the dark web."[128] The easily obtainable state voter file (available for purchase for $20[129]), SURE's polling place location tool (accessible via the Internet[130]), and leaked fundraising and voter file information and credentials[131] could further aid would-be attackers looking to target SURE.[132]

Armed with voters' personal information, attackers could create fake registrants or modify existing records by changing names, addresses, or party affiliations. Fake registrations would have little impact, of course, without individuals attempting to vote under the fake registration records—such a scheme at a scale sufficient to affect the outcome of an election would present some logistical challenges but could succeed depending on the margin of victory relative to the attack's scale.

Similarly, Harvard University researchers in a 2017 paper argued that hackers could mount a coordinated campaign of voter identity theft in targeted states, submitting false changes to actual voter records, albeit through a laborious process of changing individuals' information one at a time.[133] The authors determined that it would cost $315 to obtain voter information and then, through automation, attack the voter database in a way that would alter 10% of the vote in Pennsylvania.[134] Election officials strongly disputed some of the paper's findings, stressing that safeguards—like automated security features of registration websites and other measures to detect and prevent bulk changes to voters' registration records—were already broadly in place across the country.[135]

Threat Scenario

Hackers working at the direction of a foreign adversary could purchase the Pennsylvania state voter file for $20 from the Department of State. The hackers could then purchase on the dark web driver's license and/or social security numbers for adult Pennsylvanians of voting age and glean further useful information from the SURE polling place lookup tool.

Then, relying on historical turnout, polling, and predictive data about competitive elections from sites like FiveThirtyEight and local media outlets, the hackers could pinpoint which precincts and areas to target with fake, deleted, or changed registrations. The goal: to create enough chaos in selected precincts to depress turnout in a way advantageous to favored candidates.

This type of attack also has the benefit of eroding confidence in election administration—a likely goal of an adversary.

The vulnerabilities that both sets of researchers identified are similar in nature: Hackers could exploit publicly available information coupled with ill-gotten personal information to effect changes in Pennsylvania's voter registration records.

Most experts agree that nefarious changes to registration records of the volume needed to impact election outcomes would be identified before Election Day. But it might not be possible to correct all maliciously altered information before voting, potentially leading to long lines at polling places, increased use of provisional ballots, and public doubt in the voting process. Even if election officials would be able to take appropriate remediation before voting commenced, such an attack could still have an impact on confidence in the vote and create substantial administration headaches for officials.

DDoS Attacks

Another key threat is a DDoS attack on public-facing voter registration websites and election results reporting websites. This type of attack "occurs when multiple machines are operating together to attack one target ... [and] allows for exponentially more requests to be sent to the target, therefore increasing the attack power ... [and] the difficulty of attribution, as the true source of the attack is harder to identify."[136] Such an attack could prevent "voters from registering and potentially discourag[e] them from participation."[137] It could also disrupt election-night reporting of preliminary, unofficial election results.

To be sure, the threats to and vulnerabilities of Pennsylvania's voter registration system are sobering. Successful attacks to the system could create substantial administrative challenges for election officials and frustrate voters in a way that could depress turnout. And such an attack could undermine faith in the Commonwealth's elections and erode public trust in democracy—outcomes that must be prevented.

HOW CAN PENNSYLVANIA IMPROVE THE SECURITY OF THE VOTER REGISTRATION SYSTEM?

The process to replace SURE will likely present challenges—but also an opportunity to shape a modern, secure, and user-friendly system that should serve Pennsylvania for years to come. In addition, by implementing cybersecurity best practices where not already in place, officials can shore up existing weaknesses to improve cyber defenses.

Recommendation 3: Implement Cybersecurity Best Practices throughout Pennsylvania's Election Architecture.

Review and, where not already in place, implement cybersecurity best practices across Pennsylvania's election architecture.

As noted in the sections above concerning election management systems, officials should institute basic cybersecurity best practices, where they have not already been instituted, throughout Pennsylvania's election architecture.

Implement multifactor authentication before implementing changes to a registration record in SURE.

With respect to the SURE system specifically, implementation of multifactor authentication could mitigate a specific vulnerability discussed above—namely, the nefarious alteration of registration records without voter knowledge. The Department of State should consider such an authentication method, presumably by verifying a piece of information that is provided upon application for registration. It is important to consider the impact of any added layers of security on the ability of eligible voters to make changes to registration records online without undue burden.

Add an additional layer of encryption to SURE system data.

In addition, the Department of State should consider adding a second layer of encryption to data in the SURE system. At present, data are stored on encrypted hardware behind a layered set of protections/controls designed to prevent any malicious actor from accessing data. A second level of encryption would further protect registration system data by encrypting the data within the encrypted hardware.[138]

Send paper notifications to registered voters after online changes to records.

The commission also recommends requiring that officials mail paper notification letters to registrants on Pennsylvania's online voter registration application who change their records. For registrants changing an address, officials should send a letter to both the old and the new address.

Require mandatory pre-election testing of e-pollbooks across Pennsylvania (where e-pollbooks are used) to ensure e-pollbooks are in good and proper working order before Election Day.

With respect to pollbooks, the commission recommends mandatory pre-election testing of e-pollbooks (where they are used) to ensure e-pollbooks are in good and proper working order before Election Day. The commission further recommends that officials continue the current practice of limiting wireless communication between e-pollbooks and locations outside the precinct.

Recommendation 6: Follow Vendor Selection Best Practices in SURE Replacement Procurement and Leverage Auditor General's Findings.

In connection with the upcoming procurement process to replace SURE, the Department of State should heed vendor selection best practices applicable to election infrastructure.

The procurement process to update and replace SURE will give Pennsylvania a prime opportunity to improve the security, reliability, and function of the statewide voter registration system. Department of State personnel responsible for this procurement should seize this opportunity to develop an improved voter registration system that incorporates cybersecurity best practices while heeding guidance from subject-matter experts about how best to select and manage vendors.

There are several sources that Pennsylvania officials can consult to help guide vendor selection and management. For example, the U.S. Department of Homeland Security has offered salient guidance in a document titled *DHS Election Infrastructure Security Funding Considerations*.[139] Relatedly, the Center for Internet Security's handbook includes a helpful "Code of Practice for Information Security Controls" to govern supplier relationships.[140] The U.S. Election Assistance Commission provides examples of local purchasing contracts with language about security expectations that counties can use as templates.[141] The Department of State personnel involved in

Pennsylvania's voter registration system presents vulnerabilities that could put the integrity of—and public confidence in—the Commonwealth's vote at risk.

this procurement process should consider these materials, and others,[142] as well as the vendor questionnaires developed by the County Commissioners Association of Pennsylvania. The Department of State should leverage the contracting process to require any vendor to adhere to either the Commonwealth's information technology policies or the specific guidelines in the reference documents cited in this report.

In particular, the Department of State should ensure that the Commonwealth retains ownership of any software code developed in the replacement of the SURE system. If possible, the Department should require that the system be developed with an open-source software platform, or disclosed-source software, so that the Department can control and implement its own schedule of risk and vulnerability testing of that software periodically through the lifecycle of the system. An open source or disclosed source system will remove the barrier of obtaining permission to examine proprietary code. Vendor(s) should be required to notify the Department of State of any defect, fault, or failure of any system services provided by the vendor(s); should be obligated to submit to regular penetration testing; and should face a mandate to keep software current through updates and security patches.

Beyond the SURE procurement process, the State and counties should be conscious of supply chain vulnerabilities.

Beyond the voter registration system procurement process, state and county officials should follow best practices in dealing with vendors that affect the election architecture. It is imperative that election officials remain conscious of supply chain vulnerabilities and assess contractors or vendors for security risks. All contractors or vendors should be assessed for security risks. Security considerations should be a key selection factor—not reviewed after a procurement decision has been reached.

The Department of State should work closely with the Auditor General's office in connection with that office's audit of Pennsylvania's voter registration system. Any relevant audit findings should be taken into account in the upcoming procurement process.

Lastly, the commission believes that voters would be well served by Pennsylvania officials working together to leverage the Auditor General's efforts to audit the voter registration system in particular, as well as voting systems in general. To that end, the commission urges the Department of State to work closely with the Auditor General's office in connection with the audit. Close collaboration and cooperation could arm Department of State personnel with detailed knowledge about any audit findings that could inform the SURE procurement process or bolster the cybersecurity of other components of the Commonwealth's election infrastructure. Moreover, the commission urges close consultation with the Inter-Agency Election Preparedness and Security Workgroup and the county/Commonwealth election security workgroup.

Pennsylvania's voter registration system presents vulnerabilities that could put the integrity of—and public confidence in—the Commonwealth's vote at risk. Common sense, cybersecurity best practices can mitigate many of these risks. And the upcoming procurement process to replace SURE presents an excellent opportunity to bolster the security of Pennsylvania's statewide voter registration system.

Post-Election Tabulation Audits

Overview

Without ... a paper record, it is impossible to conduct robust, post-election audits.

Pennsylvania's paperless voting machines are perhaps the weakest link in the cybersecurity of the Commonwealth's election architecture. As noted elsewhere in this report, most Pennsylvanians vote on machines that lack an auditable paper trail (i.e., paperless DRE machines). Without such a paper record, it is impossible to conduct robust, post-election audits. Consequently, this inability to conduct meaningful post-election audits of election results aggravates the security vulnerabilities that paperless DRE machines pose in Pennsylvania. The Department of Homeland Security Secretary rightly characterized this state of affairs as a "national security concern"[143] and has "called on all election officials to ensure that every American votes on a verifiable and *auditable* ballot by the 2020 election."[144]

As the commission has recommended, Pennsylvania officials should, of course, replace vulnerable paperless machines. Pennsylvania officials must also—in connection with replacing vulnerable paperless DRE machines—implement mandatory, statistically sound post-election audits for every race. Such measures, which experts widely agree are best practices, would do much to shore up the resilience of Pennsylvania's elections and arm officials with the means of both detecting and recovering from attacks or errors affecting the tabulation of votes.

LACK OF MEANINGFUL AUDITABILITY

All computers can suffer from exploitable vulnerabilities, whether paperless DRE machines or optical scan systems. And although officials can take many wise and prudent steps to prevent the compromise of the computers that count votes, many of which the commission has recommended in this report, it is impossible to prevent *every* type of possible attack or error affecting voting machines. Officials can, however, take action to arm themselves with the means of detecting such issues.

At first blush, the Election Code seems to do just that.

Pennsylvania law requires a recount of a random sample of the lesser of either (i) 2 percent of votes cast in a county or (ii) 2,000 ballots.[145] Yet most Pennsylvania counties use paperless DRE machines, leaving officials unable to perform this required audit beyond re-tabulating the vote counts that DRE machines provide. Because there are no individual voter-marked ballots to check, officials lack the means to audit the machines' ability to correctly interpret and preserve voters' intent. A recount of a paperless voting machine cannot catch corrupted records, whether tainted by malicious intent or benign error.

Put simply, without individually marked ballots to audit, election officials cannot meet the Election Code's requirement of a recount with paperless DRE machines.

HOW CAN PENNSYLVANIA IMPROVE THE AUDITABILITY OF ELECTION TABULATIONS?

Recommendation 7: Employ Risk-Limiting Audits.

Pennsylvania should employ transparent risk-limiting audits after each election.

The commission recommends implementing risk-limiting audits after every election to determine whether reported results from voting machines and tabulation systems included any errors. Election security experts widely agree that voter-marked paper ballots paired with risk-limiting audits are the "gold standard" in tabulation security.[146] Risk-limiting audits performed before certification will meet the criteria of the recent settlement agreement in *Stein v. Cortes*, referenced above. As University of Pennsylvania computer scientist Matt Blaze has described, "[t]he effect of risk-limiting audits is not to eliminate software vulnerabilities, but to ensure that the integrity of the election outcome does not depend on the Herculean task of securing every software component in the system."[147]

These risk-limiting audits, in which officials check a random sample of paper ballots against digital tallies to ensure the results were tabulated without error, allow officials to detect software failures and attacks, including those that might have been initiated within the supply chain.[148] According to a seminal paper on risk-limiting audits, "[a] risk-limiting audit is a method to ensure that at the end of the canvass, the hardware, software, and procedures used to tally votes found the real winners."[149] Although risk-limiting audits "do not guarantee that the electoral outcome is right," they do "have a large chance of correcting the outcome if it is wrong."[150] Here "right" and "wrong" are defined relative to what an accurate hand count of paper ballots would show.

A sample size is chosen to provide strong statistical evidence that the reported outcome of an election is correct—and a high probability of identifying and correcting an incorrect outcome. The margin of victory in the race and the chosen "risk limit," which specifies the minimum chance of finding and correcting an incorrect a tabulation outcome if a full hand count of the paper record would change that outcome, both drive the determination of the number of ballots that officials must count in a risk-limiting audit.

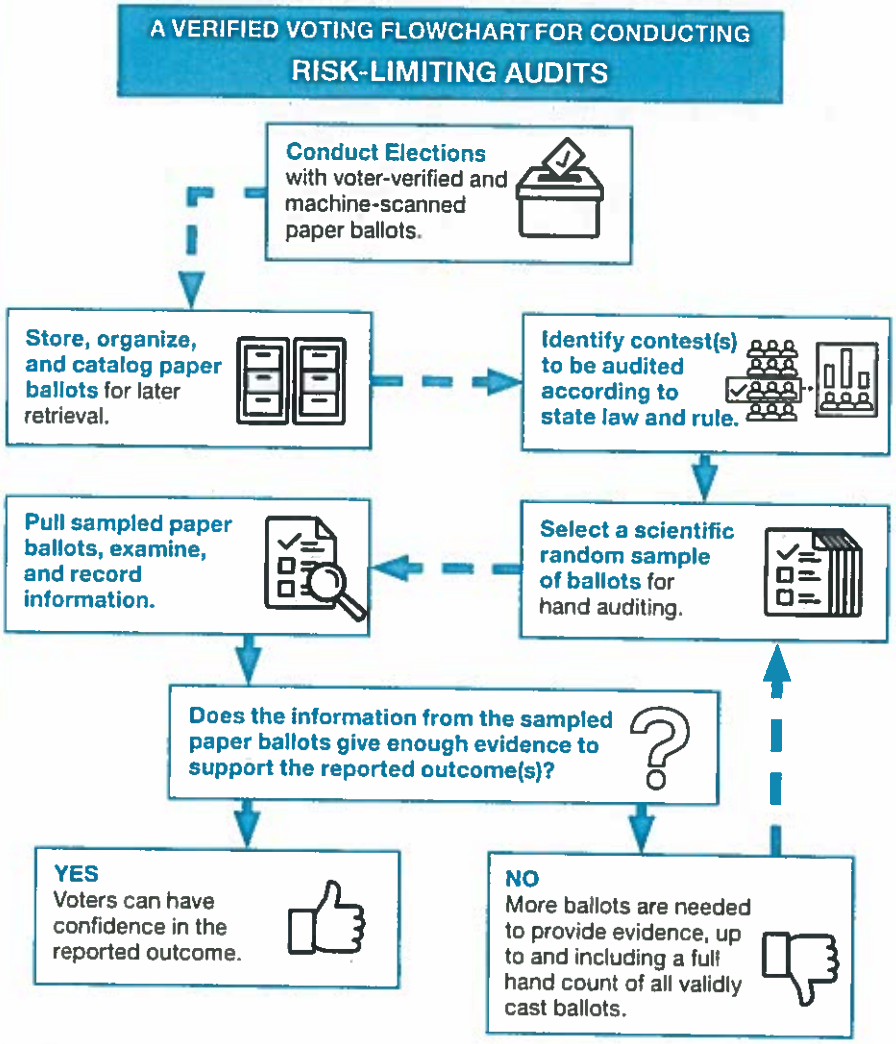
Risk-limiting audits are preferable to the audits that Pennsylvania law currently requires, "which require a set number (or percentage) of ballots to be counted," because risk-limiting audits can provide "a high level of confidence in the results while generally requiring fewer ballots to be hand counted than what is already required in many states using traditional audits."[151] This efficiency can make risk-limiting audits less expensive than traditional audits, delivering a potential cost savings to election officials. According to an analysis of Colorado's 2017 announcement that it would implement risk-limiting audits, *Politico* reported that "a regular [i.e., statutory fixed percentage] audit of the 2016 presidential election results in Colorado would have required counting more than 32,000 paper ballots out of 2.85 million votes statewide. That number [would] drop to 142 with the new risk-limiting audit software, according to Stephanie Singer, the project lead at Free & Fair."[152] And according to a recent white paper by the U.S. Election Assistance Commission, "[m]ost counties in Colorado experienced a time savings after conducting [risk-limiting audits] for the 2017 Coordinated Election compared to their previous random machine audit."[153]

Risk-Limiting Audits: How Do They Work?

"Statistical principles determine the size of the sample—but, in plain terms, more ballots are counted in a close race, while a race with a larger margin would require fewer ballots to be counted. If testing of the sample is consistent with the original vote total, it is almost certain that the initially declared winner won the race. If, on the other hand, the sample has substantial discrepancies with the original tally, the audit continues until there is 'sufficiently strong statistical evidence that the apparent outcome is right, or until all the ballots have been manually counted.'"

Commission Staff Christopher Deluzio, "A Smart and Effective Way to Safeguard Elections," Brennan Center for Justice Blog, July 25, 2018

Risk-limiting audits can provide another advantage: Traditional audits (such as fixed-percentage audits) run a large risk of failing to detect an incorrect outcome in an election. Because those audits may call for sampling "whole precincts or other large batches of ballots," they might miss errors that "are clustered in only a few precincts."[154]



Source Verified Voting
https://www.verifiedvoting.org/wp-content/uploads/2018/10/VV-RLA-Flowchart-731x1024.png

Although there are several types of risk-limiting audits, in essence, they are all designed to provide strong evidence that tabulation errors have not altered outcomes in particular contests. A risk-limiting audit continues until strong evidence exists that the tabulation outcome was not incorrect—or, if necessary, a full hand count is conducted to determine the correct outcome. Officials can stop a risk-limiting audit "as soon as it finds strong evidence that the reported outcome was correct."[155]

RISK-LIMITING AUDIT METHODS

RLA Method	Description
Ballot-level comparison	Individual ballots are randomly selected and compared to the voting system's cast vote record (CVR) for each ballot.
Batch-level comparison	Batches of ballots are randomly selected and compared to batch subtotals produced by the voting system.
Ballot-polling	A random sample of ballots are selected and the results for the selected contest(s) are tallied; the audit stops if it produces strong enough evidence to support the reported outcome.
Batch-polling	A random sample of batches are selected and the results for the selected contest(s) are tallied; the audit stops if it produces strong enough evidence.

Source: U.S. Election Assistance Commission
https://www.eac.gov/assets/1/6/Risk-Limiting_Audits_-_Practical_Application_Jerome_Lovato.pdf

There is growing momentum across the country to embrace risk-limiting audits.

Colorado instituted the requirement that all elections be subject to a risk-limiting audit,[156] becoming the first state to carry out mandatory post-election audits in 2017.[157] The open-source audit software used in Colorado is available for free and can be customized for other states.[158] Rhode Island also passed a bill requiring risk-limiting post-election audits for future elections.[159] Both states provide good examples that could be used, with some adaptations, for Pennsylvania's particular election requirements. And examples of pilot risk-limiting audits abound in, for example, jurisdictions in California, Indiana, Michigan, and Virginia.

Risk-limiting audits, which officials should implement transparently and for every election, are critical to building confidence in Pennsylvania's elections. They could be a potent defense in the face of threats of attacks or disinformation campaigns.

The Department of State, in partnership with select counties, should pilot risk-limiting audits. The General Assembly should then pass legislation to make this a statewide requirement.

Recent action by the Department of State suggests potential recognition of the value of risk-limiting audits.

In the Commonwealth's settlement of presidential candidate Jill Stein's lawsuit challenging Pennsylvania's recount procedures and use of DRE voting systems, among other things, Pennsylvania officials agreed to certain measures related to implementation of post-election audits. In particular, the Department of State agreed to "direct each county to audit all unofficial election results using robust pre-certification audit methods to be determined based on the recommendations of a Work Group established by the Secretary."[160] Per the agreement, the Work Group's recommendations must be "consistent with applicable statutory authority" and certain specified principles, and the Work Group's report is due by January 1, 2020.[161] The Department of State further agreed to direct pilot audits to occur in 2021, with full implementation by the 2022 general election.[162]

Replacing vulnerable voting equipment (DREs) should be Pennsylvania officials' top priority in working to secure the Commonwealth's elections.

Yet the agreement still leaves much to be done to implement risk-limiting audits for every election. First, nothing in the agreement *requires* the Commonwealth to utilize risk-limiting audits—the "gold standard" of post-election audits. Moreover, the agreement calls for audits that are "consistent with applicable statutory authority"—yet, as noted above, the Election Code requires recounting a random sample of the lesser of either (i) 2 percent of votes cast in a county or (ii) 2,000 ballots.[167] Consequently, the settlement agreement does not seem to contemplate risk-limiting audits, absent a revision to the Election Code by the General Assembly.

The commission therefore urges the General Assembly to mandate risk-limiting audits for every election in Pennsylvania (coupled with the adoption of voter-marked paper ballots across the Commonwealth). In addition, the Department of State should pilot risk-limiting audits in partnership with counties that already use optical scan voting systems, ideally on a more expedited timeline than required by the settlement agreement. In parallel to those pilot efforts, the Department of State should develop uniform procedures for risk-limiting audits based on the experience during pilots and the Work Group's report.

Replacing vulnerable voting equipment (DREs) should be Pennsylvania officials' top priority in working to secure the Commonwealth's elections. Yet any effort to improve election security in Pennsylvania would be incomplete without mandating robust, post-election audits for every race. Risk-limiting audits are the "gold standard" of such audits, and Pennsylvania should take steps to implement them without delay.

Recovery and Resilience

Overview

Yet cyber threats are constantly evolving, making it all the more important for election officials to constantly scrutinize and assess relevant contingency planning for election systems, including how to recover from technological attacks, malfunctions, or errors.

The cyber threats to our election infrastructure have garnered significant attention in the press, in government, and among policy experts. That attention has laudably prompted officials to take action to *prevent* cyberattacks on our elections. But officials' efforts to contend with the fallout of an attack have received far less scrutiny. Such contingency planning is central to building and maintaining a resilient election system capable of recovering in the face of efforts to undermine our democracy—whether through a direct attack on election systems or an indirect attack on the power grid or some other piece of infrastructure with a nexus to voting.

Election officials in the United States have a history of focusing on contingency planning, thereby providing a measure of strength in the American election system. Indeed, the U.S. Senate Intelligence Committee's investigation into Russian targeting of election infrastructure during the 2016 election reviewed state and local election security planning and "concluded that U.S. election infrastructure is fundamentally resilient."[164] Yet cyber threats are constantly evolving, making it all the more important for election officials to constantly scrutinize and assess relevant contingency planning for election systems, including how to recover from technological attacks, malfunctions, or errors.

Such planning could be the difference between a seamless recovery and a disruption of voting in the event of cyberattack or other technological issue. According to Pam Smith, past president of Verified Voting: "Well implemented emergency procedures can make the difference between a jurisdiction that's all over the news as an epic fail, or a jurisdiction that had a few issues that were resolved, and everyone got to vote."[165] And as the U.S. Election Assistance Commission has observed, "[t]he number of attempts to infiltrate computer systems rises every day," and in the event of such an attack, "the greatest risk is to not have policies and plans to respond to the incident."[166] Thus, at its core, proper contingency planning will allow voters to exercise the franchise on Election Day—and to have votes counted correctly—in the face of technological attacks or failures. Proper planning and related communications should enhance Pennsylvania voters' confidence that their votes are being counted, even amidst an attack, and that election administration is proceeding as described by election officials in public communications.

Pennsylvania officials have demonstrated an appreciation of the importance of good contingency planning to bolster resilience.

Commonwealth and county election personnel took part in the "Tabletop the Vote 2018 exercise" with the U.S. Department of Homeland Security in August 2018, billed as a "first-of-its-kind national and local election cyber exercise,"[167] as well as a state-led tabletop exercise in September 2018.[168] In addition, many sound contingency measures are reflected in the Election Code, Department of State guidance, and election practice: the existence of cyber incident response plans, adequate supplies of paper ballots in polling places that use them, adequate supplies of emergency backup paper ballots in places that use paperless machines, and e-pollbook paper backups, for example. And the Commonwealth's voter registration system has several measures in place to ensure its recoverability and to bolster its resilience in the event of an attack or other calamity. Nonetheless, officials could improve planning in certain areas. Given the high price of restoring voter confidence once lost, these measures are commonsense investments in democracy in Pennsylvania.

PENNSYLVANIA'S RELEVANT CONTINGENCY MEASURES

This section addresses key elements of contingency planning that are central to the resilience of Pennsylvania's election systems: Cyber Incident Response Planning, Voting Equipment, E-pollbooks, Voter Registration Systems, and Election-Night Reporting Systems.[169]

Cyber Incident Response Planning

In light of today's cyber threats and the documented efforts by nation-state rivals to target election systems, election officials must plan for and have ready a cyber incident response plan. Such a plan documents "a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyberattack against an organization's information systems(s)."[170] Much like contingency planning for threats to physical infrastructure, election officials "should understand critical election system vulnerability points and create a detailed response plan (both internal processes and communications) for any system compromise."[171] A robust communications plan is a critical element of any good plan and should be "intended to assist election officials in distributing essential information in a timely manner and retaining public confidence in the election administration system."[172]

Given the sensitive nature of cyber incident response planning, election officials in Pennsylvania (at the Department of State and in several counties contacted by commission staff) declined to share specific policy documents, pre-planned responses, communications plans, or other information that would enable the commission to assess the adequacy of the Commonwealth's planning. Understandably, such materials are not publicly available, lest adversaries (nation-state or otherwise) gain valuable intelligence about how election officials might respond to attacks.

Consequently, there is little to report on the planning in place within the Department of State and Pennsylvania's counties. However, Department of State personnel provided some information about Pennsylvania's cyber incident response planning, including the following:

- Planning is updated before each election, if not more frequently as needed.
- Federal and local partners are regularly consulted for feedback, which is integrated into planning.
- Best practices (such as those put forward by the Center for Internet Security) are heeded in cyber incident planning.
- The Department of State has issued relevant guidance to counties.
- Communications planning (including responses to disinformation campaigns) is part of the Commonwealth's cyber incident response planning.[173]

Natural Disasters and Other Emergencies

Loss of power, whether by cyberattack or natural disaster, such as a severe storm or tornado, could also disrupt or disable Election Day voting operations, shutting down polling places in Pennsylvania.

To guard against a loss of power, Bucks County, for example, provides multiple diesel and natural gas generators that could provide power to polling places if necessary. County administrative offices also have uninterruptible power supplies to ensure continuity of operations.

Yet such preparations could be overcome by disaster-level power outages, weather conditions, or widescale cyberattacks preventing voters from traveling to the polls.

As discussed later in this section, the Election Code should provide clear procedures and authority for suspending or extending an election in the event of an emergency (caused by severe weather or otherwise, including, for example, a cyberattack against electric grids).

Voting Equipment

Voting equipment—like any similar technology—can experience failures. Whether due to a malicious attack, improper upkeep, or an unexpected malfunction, voting equipment is susceptible to a range of issues that could affect machine effectiveness and voting on Election Day.

The most significant deficiency in Pennsylvania is the dominance of DRE systems that have no paper record. As of November 2018, fifty of sixty-seven counties in Pennsylvania were relying on paperless DRE systems, which lack resilience; even if an attack or error could be detected, there is typically no way to recover from such events with paperless systems. Similarly, DRE machines can be more likely to create voting disruptions than paper-based systems. In the event of DRE breakdown or failure, "voters may have to wait in long lines while election workers scramble to repair them."[174]

Although the Commonwealth has taken laudable steps to replace these paperless machines by the end of 2019, the machines remained prevalent in Pennsylvania during the 2018 midterm election and could still be in use in the 2020 election.

Paper-based voting systems, on the other hand, can be less affected by machine malfunctions. For polling places using optical scan machines, for example, "voters can fill out paper ballots even if machines are not functioning, and the ballots can be ready after the scanners are replaced or fixed."[175]

Pennsylvania has several measures in place relevant to voting equipment issues.

In the event of a failure of "any electronic voting system or any component thereof" during voting, the Pennsylvania Election Code authorizes the use of emergency backup paper ballots if the equipment cannot be repaired or replaced.[176] According to a Department of State directive interpreting this provision, emergency backup paper ballots "shall be distributed immediately to eligible voters ... [i]f 50% of electronic voting machines in a precinct are inoperable."[177]

Emergency backup paper ballots are cast as regular ballots and "shall be deposited by the voter in a ballot box or other secure receptacle designated by the board of elections for the deposit of completed emergency back-up paper ballots, as required for paper ballots by Section 1003(a) of the Election Code, 25 P.S. §2963(a)."[178] The directive required county election boards to "supply an adequate amount of emergency back-up paper ballots"; a subsequent directive advised that the Department of State "believe[s] that providing to each election district a number of emergency paper ballots equal to **20% of the number of registered electors in each district** is a reasonable formula for determining how many emergency paper ballots to make available on location at each election district."[179]

In addition to emergency paper ballots, the Department of State has determined that county boards of elections may use "surplus, un-voted absentee ballots; surplus, un-voted alternative ballots; ballots that

Primer on Ballot Types

Regular ballots: typical ballots cast by eligible voters on Election Day; voters cast paper ballots in polling places using paper ballots or vote on DRE machines where they are used.

Absentee ballots: paper ballots cast before Election Day by eligible voters who will be absent from the polling place on Election Day. Absentee ballots are sent to county boards of elections.

Emergency paper ballots: paper ballots provided to eligible voters if DRE voting machines fail during voting on Election Day.

Provisional ballots: ballots provisionally cast by voters when, for example, there is some question about their eligibility to vote that must be resolved before counting their ballots.

Alternative ballots: paper ballots cast by eligible voters with a disability or those older than 65 years whose polling places are not accessible; they are cast before Election Day and sent to county boards of elections.

the county board of elections has supplied to the district election board for use as provisional ballots; or other paper ballots that are 'either printed or written and of any suitable form.'"[180] Thus, counties have a range of ballot options in the event that voting machines fail and cannot be restored (or replaced) for voting; however, officials should avoid using provisional ballots as emergency paper ballots for eligible voters in light of the confusion and added procedural hurdles associated with provisional ballots.

For polling places using paper ballot–based voting, the Election Code requires county election boards to have ballots in excess of the total relevant registered voters in each precinct.[181] Counties must also "maintain a sufficient supply of such ballots at the office of the county board for the use of absentee electors and for the use of any district, the ballots for which may be lost, destroyed or stolen."[182] Having ballots sufficient for 100% of registered voters (or affiliated voters in the case of a primary election) should prevent ballot shortages, particularly when turnout exceeds historical turnout in like elections (as happened in the 2018 midterm elections),[183] although this requirement will undoubtedly lead to excess ballot preparation. The ability to print and deliver extra ballots (as Philadelphia successfully did during the high-turnout 2012 general election) is also a safeguard.

In another key requirement, Pennsylvania election officials must conduct logic and accuracy testing on voting equipment before Election Day[184]—an important measure to detect issues and reduce the likelihood of equipment issues during voting. Note, however, that such pre-testing cannot by itself ensure correct equipment behavior during the processing of actual ballots.

Poll workers are perhaps the most important on-the-ground personnel on Election Day when it comes to executing elections and implementing contingency measures. In that sense, poll workers are critical to maintaining continuity of operations in polling places. Training such personnel, consequently, is imperative, and county officials must prioritize robust training. The Department of State makes available on its website poll worker training videos on a range of topics such as opening the polls, processing voters, and closing the polls.[185] In addition, the Department of State provides a training video about assisting voters with disabilities.[186]

The training videos are directed to generic election officials and are not tailored to specific counties or the equipment in use in each county or polling place. Counties also provide training for poll workers, often using county-specific materials.[187] However, most counties do not have the legal authority to require poll workers to attend trainings, something officials ought to consider implementing.

E-pollbooks

Several Pennsylvania counties use electronic pollbooks (e-pollbooks). E-pollbooks are subject to a Department of State test protocol[188] and certification for use in Pennsylvania.[189] That process includes "conformance to statutory requirements," "review of system capabilities," and "compliance with Commonwealth [information technology] policies."[190]

The Department of State's poll worker training videos address voter check-in using paper pollbooks (but not e-pollbooks).[191]

According to the Department of State,[192] counties using e-pollbooks have backup paper pollbooks in polling places. This is an important requirement that provides the

Even when first-line defenses are good, contingency planning measures are necessary to mitigate the harm of any successful attack.

best alternative in the event of e-pollbook failure. Having backup paper pollbooks at the ready in polling places allows "poll workers to continue confirming eligibility of voters, minimize[s] the potential for long lines, and may minimize[s] the need to issue provisional ballots."[193] For example, Durham County, North Carolina experienced e-pollbook failures in November 2016 and, as a result, voting delays as long as an hour and a half while poll workers waited for paper pollbooks to arrive.[194] Poll workers may also contact county officials to determine voter eligibility, if need be.

Yet even where backup paper pollbooks are available in polling places, it may not be possible to determine voter eligibility to cast a regular ballot. For example, if e-pollbooks fail *during* voting and poll workers are unable keep track of which voters have voted throughout the day, backup paper pollbooks may not be sufficient to determine whether someone had voted earlier on Election Day. In such situations, it may be necessary for poll workers to issue provisional ballots to voters. Doing so ensures "individuals can cast a ballot, while providing election officials additional time to determine their eligibility."[195]

The Department of State has issued procedures for provisional balloting,[196] as well as a *Provisional Ballot Guidance Summary*.[197] Both Pennsylvania and federal law provide for the right to cast a provisional ballot, and the procedures describe scenarios where provisional voting is appropriate, as well as the process for provisional balloting.[198] The Department of State procedures recognize that an individual who claims to be registered and eligible to vote in the polling place but does not appear on the general register or whose eligibility is challenged by an election official has the right to cast a provisional ballot.[199]

Voter Registration Systems

As discussed earlier in this report, Pennsylvania's voter registration system is the Statewide Uniform Registry of Electors (SURE). That system is not only critical to processing and maintaining the list of eligible and registered Pennsylvania voters but also instrumental in helping election officials prepare pollbooks of voters for use on Election Day. For that reason, and others, a failure of the system in the lead-up to Election Day could pose a range of problems, including loss of voter lookup tools, bad data for pollbooks, and difficulty validating provisional ballots.

The Department of State employs many best practices[200] in managing the SURE system that should serve to reduce the likelihood of a successful attack on the system, including the following:

- Access control so that only authorized personnel have access to the database
- Logging capabilities to track database modifications
- Intrusion-detection system and regular vulnerability assessments
- Required cybersecurity training for Commonwealth employees (with planned requirements for local officials in the future)[201]

Yet even when first-line defenses are good, contingency planning measures are necessary to mitigate the harm of any successful attack or other technical failure, for "[i]t is impossible to defend against every conceivable attack."[202] Pennsylvania has a disaster recovery site for SURE servers and equipment that would allow recovery of the system in the event of failure or loss of the primary site. The Commonwealth also employs a pre-election blackout window for non-critical updates/patches to SURE and

maintains offline backup copies of digital records, which could be used if online access were limited. A best practice with respect to backups in the lead-up to an election is to "download an electronic copy of voter information on a daily basis and store it securely so [officials] have the most recent information in case the voter registration system becomes unavailable."[203] Pennsylvania also has a voter registration lookup tool, accessible over the Internet,[204] and regularly provides voters with election- and registration-related information via the VotesPA.com website, social media channels, and frequent press calls during voting. Counties likewise disseminate voting-related information via the Internet and social media.

These are commendable practices that should provide layers of security so that SURE will be able to recover from a disruptive event, but they do not obviate the need for robust recovery planning.

Election-Night Reporting Systems

As discussed above in the section addressing election management systems, public-facing election-night reporting websites can be susceptible to cyberattack.

For the transmission of unofficial results, Pennsylvania already employs a best practice for its election-night reporting: Unofficial election-night returns transmitted through the Department of State's Election Night Returns application must be transmitted via a county computer that is *not connected directly* to any of the components of the voting system, including the computer on which the election management system resides. This important measure "can minimize the potential that a targeted attack on the reporting system will have any lasting impact."[205] Moreover, the results displayed on election-night reporting websites are *unofficial*—thus, even if an attacker were to manipulate results on a public-facing website, the *official* results would not be affected. Of course, such an attack could sow confusion and undermine confidence in the election.

As discussed above, county and Commonwealth communications plans are the best weapon to defeat efforts to undermine trust in the vote. Such plans should include contacting social media company liaisons and/or law enforcement to report disinformation campaigns. Pennsylvania officials should also have in place a sound contingency plan for recovering from a spoofed website or DDoS attack or alteration of the reported results on the Department of State election-night reporting website.

HOW CAN PENNSYLVANIA IMPROVE CONTINGENCY PLANNING?

The threat of cyberattacks on election infrastructure is substantial and likely to increase in the short term. This reality makes contingency planning to mitigate the consequences of such an attack or other technological failure all the more important. The next page offers recommendations for officials to bolster such planning in the Commonwealth to ensure that a successful election can occur even in the face of a cyberattack.

Recommendation 8: Implement Best Practices throughout Pennsylvania's Cyber Incident Response Planning.

Given the limitations on what officials shared with the commission, there is limited visibility into the *substance* of existing cyber incident response planning. Nonetheless, the commission presents some resources with best practices that those charged with Pennsylvania's election cyber incident response planning ought to consider.

Review and, where not already in place, incorporate cybersecurity best practices into Pennsylvania's cyber incident response plans.

As noted above, the commission was unable to meaningfully assess the substance of Pennsylvania's cyber incident response planning. Understandably citing the sensitive nature of those plans, Pennsylvania officials declined to share details and documents with the commission. Nonetheless, Pennsylvania officials—at the county and state levels—should consider and, where not already in place, implement best practices for planning. To that end, several excellent resources are available.

The U.S. Election Assistance Commission published *Cyber Incident Response Best Practices*, which the Commission developed in collaboration "with election officials and other partners to provide best practices on topics of interest to the election community."[206] The document includes an "Incident Handling Checklist," with steps devoted to detection and analysis; containment, eradication, and recovery; and post-incident activity.[207]

The U.S. Department of Homeland Security provided election officials with another useful resource: *Incident Handling Overview for Election Officials*.[208] The document provides contact information for the National Cybersecurity and Communications Integration Center, which can provide cyber incident response services through its Incident Response Team, as well as a checklist for seeking such assistance.

Harvard's Belfer Center published a more detailed resource, *The Election Incident Communications Plan Template*, which "is primarily intended for use by state and local election officials as a basis for developing their own communications response plans, which include best practices for use in an election cyber incident."[209] The template is customizable for a jurisdiction's unique needs and, thus, can be tailored to specific county or state requirements—and it pays substantial attention to the communications aspects of cyber incident response planning, something that would be vital to managing the fallout of a cyber incident on Election Day. Officials can also use the document in conjunction with the Belfer Center's *The Election Cyber Incident Communications Coordination Guide*, a resource designed "to coordinate multiple voices (and multiple facts) in an election cyber incident that crosses traditional jurisdictions."[210]

Such communications planning in Pennsylvania must include planned response to one type of threat in particular: disinformation campaigns. Such a campaign might include the deployment of bots or coordinated accounts on social media to spread false information about where to vote, voting hours, and the like. Relevant officials need to be ready to contact social media companies to alert them to such a campaign, have a reliable and widely known set of social media accounts to rebut disinformation, and use traditional communications means to assure the public that voting has not been disrupted.

All Pennsylvania counties should join the EI-ISAC (Elections Infrastructure-Information Sharing and Analysis Center).

Along those lines, information sharing is a key element of ensuring that the right people have the right information about threats affecting our elections. Yet, as of January 4, 2019, only five Pennsylvania counties were members of the EI-ISAC (along with the

Department of State)[211]. The EI-ISAC is a critical cybersecurity resource that assists with cyber incident responses, real-time cybersecurity advisories and alerts, and more. Perhaps most importantly, the EI-ISAC includes information sharing through the Homeland Security Information Network portal. The EI-ISAC also provides a "Cyber Incident Checklist" to help officials navigate their handling of an incident.[212] These are *no-cost* resources that every county in Pennsylvania should be using.

The federal government, including the Department of Homeland Security, should continue to build upon existing efforts to quickly and efficiently share cyber threat information with local and state election officials. Sharing information through the EI-ISAC and working to provide security clearances to election officials are good examples of how to keep election officials informed of relevant threats.

The Pennsylvania Auditor General's audit and the Commonwealth's Inter-Agency Election Preparedness and Security Workgroup should examine cyber incident response plans.

In addition, two efforts already underway in Pennsylvania present an opportunity for review of cyber incident response planning. First, the scope of the Pennsylvania Auditor General's audit of Pennsylvania's voter registration systems and voting systems should encompass cyber incident response planning. Second, and relatedly, the Commonwealth's Inter-Agency Election Preparedness and Security Workgroup should examine cyber incident response plans as part of its work to "further strengthen election security protections" in the Commonwealth.[213] Commonwealth officials are conducting both efforts, and, consequently, it should not be problematic to share sensitive information about cyber incident response plans with those officials.

The General Assembly should provide funding support to counties to bolster election-related contingency planning measures as part of a broader appropriation to support improving election security across the Commonwealth.

The commission urges the General Assembly to provide funding support to counties to facilitate improved contingency planning. Legislators should include this funding together with a broader appropriation to support improved election security in Pennsylvania.

Recommendation 9: Revise the Election Code to Address Suspension or Extension of Elections Due to an Emergency.

Pennsylvania's laws do not explicitly address an emergency situation disrupting the execution of an election. As the Commonwealth Court observed in 1987, "neither the Pennsylvania Constitution nor the Election Code ... expressly provides any procedure to follow when a natural disaster creates an emergency situation that interferes with an election."[214]

That court dealt with the question of whether a Court of Common Pleas had the authority to suspend an election due to an emergency (flooding, specifically). Although the court recognized the absence of any clear statutory authority, the court nonetheless found that:

> [T]he language of 25 P.S. § 3046 implicitly grants the court authority to suspend voting when there is a natural disaster or emergency such as that which confronted voters in Washington County on the election date here involved. To permit an election be conducted where members of the electorate could be deprived of their opportunity to participate because of circumstances beyond their control, such as a natural disaster, would be inconsistent with the purpose of the election laws.[215]

The Election Code should provide clear authority for the suspension or extension of elections due to a wide-scale cyber-related attack, natural disaster, or other emergency that disrupts voting. The Election Code should include straightforward procedures governing the declaration of an emergency and the suspension or extension of voting.

Notwithstanding this judicial decision, Pennsylvania officials would be wise to seek a revision of the Election Code to memorialize the authority to suspend or extend elections, the grounds for doing so, and the procedures to be followed in such a case.

In considering such a revision, the commission urges close collaboration among the Governor, the Department of State, the General Assembly, local election officials, and other stakeholders. A recent article in the *Emory Law Journal* surveyed other states' election emergency laws and proposed a framework that could be useful to drafters of a revision to the Election Code.[216] The proposed framework seeks "to provide clear guidance and necessary authorizations for election officials, protect voters' ability to participate in elections, and preserve the integrity of the electoral process when circumstances become particularly challenging"[217]—all interests that Pennsylvania officials should seek to serve in revising the Election Code.

The National Association of Secretaries of State's *Report of the Task Force on Emergency Preparedness for Elections* includes effective state strategies and practices—and presents results from surveys regarding approaches across the country—and may also be helpful to officials considering revision of the Election Code.[218] The revision should consider wide-scale cyber-related attacks, natural disasters, and other emergencies that could prevent the proper administration of elections. Moreover, the procedures should establish clear lines of authority for suspending a vote and erect safeguards to eliminate the possibility of partisan abuse of the procedure.

Recommendation 10: Bolster Measures Designed to Address Voting Equipment–Related Issues So Voting Can Continue Even in the Event of Equipment Failure.

Ensure that emergency paper ballots sufficient for two to three hours of peak voting are available in every polling place using DRE machines.

Paperless DRE voting systems are, by definition, not resilient. Machine breakdown or failure on Election Day may be ameliorated by a backup method of voting, but a hacking event or programming error, even if it could be detected, would likely require an election "do-over." Thus, the commission's primary recommendation of replacing DRE voting systems with resilient electronic voting systems that incorporate voter-marked paper ballots is of far greater urgency.

In any event, even regularly and properly maintained and updated equipment is susceptible to Election Day failures. And, of course, a malicious attack could impact equipment availability and readiness. Voting equipment failures can lead to voting disruptions and delays and, without adequate planning, could disenfranchise voters. Fortunately, as described above, Pennsylvania already follows many best practices related to voting equipment contingency planning. Yet officials should consider additional measures, particularly in light of the substantial vulnerabilities associated with DRE voting systems.

As described above, the Election Code as well as Department of State guidance contemplate the use of emergency paper ballots in the event of DRE machine failure. That guidance recommends that counties provide each election district with "emergency paper ballots equal to **20% of the number of registered electors in each district.**"[219]

The commission instead recommends that the Department of State amend its emergency paper ballot guidance to adopt a "2-3 hours of peak voting" measure to

determine how many ballots each polling place should have on hand. According to the Brennan Center report that recommends this metric, this allows local officials to tailor the supply more precisely based on expected voting and turnout and other factors for each election cycle. Although ballots sufficient for 20% of registered voters may very well be enough to cover two to three hours of peak voting (depending on the type of election, expected turnout, and the like), "printing enough [emergency paper] ballots for two to three hours of peak voting activity allows voting to continue until paperless DRE equipment can be repaired or replaced, or until additional emergency paper ballots can be delivered."[220] In non-presidential elections, there could also be a meaningful cost savings with the newer metric of "2-3 hours of peak voting." For example, turnout in Pennsylvania in the 2014 and 2010 midterm elections was roughly 36% and 41%, respectively.[221] Primary elections typically see even lower turnout—below 20% in non-presidential primary elections in recent years.[222]

Update poll worker training to address procedures for voting equipment failures.

Poll worker training materials should provide clear guidance about voting equipment failure procedures—including what to do if a failure occurs during voting or before voting commences on Election Day. Such training "should ensure that poll workers understand the process for counting ballots, including potential hand counting ballots, if an equipment failure cannot be resolved before voting ends."[223] Armed with that training, poll workers should thus be able to educate voters about how their ballots will be cast and counted if the usual equipment is out of service. And, of course, county officials must demand poll workers' attendance at training and competency in the covered material.

Ensure that procedures are in place to ensure that voters with disabilities will be able to vote in the event of accessible voting equipment failures.

Training should also cover topics specific to accessible voting equipment, tailored to specific equipment used in the county. Similarly, counties should ensure there are procedures in place to assist voters with disabilities and back up accessible voting equipment if accessible voting machines fail. Another option would be to provide each polling place with accessible tablets and printers for use in the event of equipment failure.[224]

Recommendation 11: Enhance Measures Designed to Address E-pollbook-Related Issues So Voting Can Continue Even in the Event of Equipment Failure.

Ensure that provisional ballot materials sufficient for two to three hours of peak voting are available in every polling place using e-pollbooks.

Although Pennsylvania provides for provisional balloting—including when a voter's eligibility is called into question (such as during an e-pollbook failure)—there is no specific requirement under Pennsylvania law governing the quantity of provisional ballot supplies that must be available in each polling place. Nicholas Weaver (a computer science researcher at the International Computer Science Institute in Berkeley, California) recommends that "every polling place ... should have enough provisional ballots for at least 20 percent of the expected turnout,"[225] whereas the Brennan Center suggests that "sufficient provisional ballots to account for two to three hours of peak voting activity will allow voting to continue in the event of system failures."[226]

Because the "two to three hours of peak voting activity" metric will give local election officials more flexibility to tailor requirements to their specific polling places, the commission recommends that the Department of State incorporate this measure into guidance and procedures. In jurisdictions that use materials for both provisional

balloting and other purposes (e.g., emergency paper ballots), officials should consider using dedicated provisional balloting materials with an adequate supply to accommodate two to three hours of peak voting.

Update poll worker training to address procedures for e-pollbook failures.

Poll worker training materials should educate poll workers about what to do in the event of e-pollbook failures. To be most effective, such training should describe when to switch to a paper backup pollbook and how to determine whether to use regular or provisional ballots. As noted above, county officials must mandate training attendance and ensure poll worker competency.

Counties using e-pollbooks should review and, where appropriate, implement cybersecurity best practices for e-pollbooks.

Counties using e-pollbooks should review and, where not already in place, implement cybersecurity best practices regarding e-pollbooks. This is especially critical for e-pollbooks that utilize wireless connectivity, as some e-pollbooks in Pennsylvania do—something that should be abandoned given the increased security risks. In addition to other best practices outlined in this report, counties should consider the following measures:

- Where wireless connectivity is used, implement proper security protocols, such as encrypted communications between e-pollbooks; strong, frequently changed passwords; and strict Election Day chain-of-custody controls.
- Confirm that e-pollbook operating system updates and software patches are received before Election Day.[227]

According to the Department of State, counties using e-pollbooks have backup paper pollbooks at the ready. But, as noted above, if e-pollbooks fail *during* voting, it may not be possible to determine whether a voter had already voted on Election Day. To address this issue, the Department of State should consider requiring e-pollbook vendors to provide devices capable of printing lists of voters who have already voted in polling places in the event that a device issue prevents voter check-in;[228] this could reduce the need to issue provisional ballots. Given the high rejection rate of provisional ballots (approximately 35% in Pennsylvania according to the U.S. Election Assistance Commission's 2016 report to Congress),[229] avoiding the use of provisional ballots can increase the likelihood that ballots cast by eligible voters will be counted.

Although there is no guarantee that every possible cyber threat or technological mishap can be prevented, election officials should take the necessary steps to ensure Pennsylvania's elections will be resilient and able to recover in the face of the most likely threats.

Many of the other issues and recommendations in this report—e.g., replacement of insecure DRE voting systems, incorporation of cybersecurity best practices, and robust post-election audits—will do much to help prevent and detect cyberattacks against Pennsylvania's elections.

Yet no defense would be complete without adequate contingency planning. Such planning can help jurisdictions respond and recover from cyberattacks or technological issues affecting elections. Although there is no guarantee that every possible cyber threat or technological mishap can be prevented, election officials should take the necessary steps to ensure Pennsylvania's elections will be resilient and able to recover in the face of the most likely threats.

Conclusion

The threats and challenges facing Pennsylvania's elections are substantial. Yet so are the stakes for democracy.

Although there is no perfect set of solutions that would protect against every conceivable cyber-related threat, the commission has identified measures that would provide robust defenses, means of recovery, and contingencies if need be. These recommendations would also serve to bolster Pennsylvanians' faith and confidence in the integrity of elections—something that would not be easily regained once lost.

The commission therefore urges Pennsylvania officials to heed calls to protect the Commonwealth's elections, something that can be accomplished only through shared commitment and collaboration at the national, state, and local levels. The voters deserve nothing less.

Frequently Asked Questions

Was Pennsylvania's voter registration system hacked during the 2016 elections?

There is no publicly available evidence that hackers gained access to Pennsylvania's voter registration system, nor is there any publicly available evidence that rules out the possibility. U.S. authorities detected efforts by nation-state actors to target several states' voter registration systems (including Pennsylvania's) during the 2016 elections.

U.S. elections are decentralized—isn't that a method of protection?

Yes, it is an important method of protection. It would be nearly impossible to directly attack the entire U.S. voting infrastructure at once. However, it would be easy to target the weakest link in a swing state's counties, to name just one example.

Furthermore, some election functions are relatively centralized. For example, most voting technology is made and maintained by only a few vendors. Attackers could target one of those companies.

In other words, decentralization may be a deterrent, but it is no defense.

The voting machines and tabulation devices are not connected to the Internet at my precinct—how could someone hack them?

Precinct-level devices are not connected to the Internet—or certainly should not be. Maintaining an air-gap is an important security measure. However, even air-gapped devices may interact with computers or devices that are or were connected to the Internet via removable media, for example, during the loading of ballot definition files (ballot building) and voting tabulation (tallying) phases through removable media. Adopting electronic voting systems that incorporate voter-marked paper ballots that are retained for recounts and audits is a critical component of a multilayered approach to cybersecurity of voting systems.

If electronic voting machines fail at my polling place, will I still be able to vote?

Yes, Pennsylvania counties using electronic voting machines must have on hand backup emergency paper ballots. If such voting machines cannot be repaired or replaced, eligible voters will be able to cast paper ballots.

Could a cyber-attack shut down Pennsylvania's elections?

Although it is impossible to predict with certainty the consequences of every possible cyberattack, election officials in Pennsylvania have many plans and measures in place that are aimed to mitigate the consequences of cyberattacks or other technological issues affecting elections. Such contingency measures—including cyber incident response planning and backup voting supplies and equipment—are important steps that can give Pennsylvania voters confidence in the resilience of elections in the Commonwealth.

Why can't I vote on my computer or through an app on my phone?

Nearly every expert who studies election security agrees that Internet voting is too vulnerable to hacking to be trusted. Hackers could target the computer, phone, tablet, or device on which a person was "casting" a vote; the wi-fi network on which the person was voting; or even the data in transmission. Even newer online voting products utilizing "blockchain" technology cannot address these (and other) security vulnerabilities and may introduce even more security weaknesses. And, of course, such online voting would present hurdles to voting for those who do not have access to reliable Internet connectivity or Internet-capable devices.

Endnotes

1 See, e.g., "Securing the Vote: Protecting American Democracy," National Academies of Sciences, Engineering, and Medicine, https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy; "Russian Targeting of Election Infrastructure during the 2016 Election, Summary of Draft SSCI Recommendations," U.S. Senate Select Intelligence Committee, https://www.burr.senate.gov/imo/media/doc/One-Pager%20Recs%20FINAL%20VERSION%203-20.pdf; "Voting Machines at Risk—An Update," Brennan Center for Justice, https://www.brennancenter.org/analysis/americas-voting-machines-risk-an-update#_ednref8; Ben Wofford, "How to Hack an Election in 7 Minutes," *Politico*, August 5, 2016, https://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144#ixzz4GTrrmQ74

2 See, e.g., "A Handbook for Elections Infrastructure Security," pp. 17–18, Center for Internet Security, https://www.cisecurity.org/wp-content/uploads/2018/03/CIS-Elections-Handbook-19-March-Single-Pgs.pdf.

3 "Russian Targeting of Election Infrastructure during the 2016 Election: Summary of Initial Findings and Recommendations," Report of U.S. Senate Select Committee on Intelligence, https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf. There was no final public report as of January 4, 2019.

4 "Securing Elections from Foreign Interference," Lawrence Norden and Ian Vandewalker, Brennan Center for Justice, p. 11, https://www.brennancenter.org/sites/default/files/publications/Securing_Elections_From_Foreign_Interference_1.pdf.

5 See "Testimony of Verified Voting: Voting System Technology and Security in Pennsylvania," Verified Voting, Marian K. Schneider, December 12, 2017, https://www.verifiedvoting.org/wp-content/uploads/2017/12/Testimony-of-Verified-Voting-12122017.pdf; "The Verifier: Polling Place Equipment in Pennsylvania—November 2018," Verified Voting, https://www.verifiedvoting.org/verifier/#year/2018/state/42. There were 11 different models of voting equipment used throughout the Commonwealth in November 2018.

6 See, e.g., "Expert Sign-On Letter to Congress: Secure American Elections," June 21, 2017, https://www.electiondefense.org/election-integrity-expert-letter/ ("Phase out the use of voting technologies such as paperless Direct Recording Electronic voting machines that do not provide a voter-verified paper ballot."); "Securing the Vote: Protecting American Democracy," National Academy of Sciences, Engineering, and Medicine, https://doi.org10.17226/25120; Testimony of J. Alex Halderman, professor of computer science, University of Michigan, before the U.S. Senate Select Committee on Intelligence, June 21, 2017, https://jhalderm.com/pub/misc/ssci-voting-testimony17.pdf; Testimony of Matthew Blaze, associate professor of computer and information science, University of Pennsylvania, before the U.S. House of Representatives Committee on Oversight and Government Reform Subcommittee on Information Technology and Subcommittee on Intergovernmental Affairs, Hearing on the Cybersecurity of Voting Machines, November 29, 2017, https://oversight.house.gov/wp-content/uploads/2017/11/Blaze-UPenn-Statement-Voting-Machines-11-29.pdf. For a partial bibliography of voting machine attack research, see J.A. Halderman, "Practical Attacks on Real-World E-voting," in eds. F. Hao and P.Y.A. Ryan, *Real-World Electronic Voting: Design, Analysis, and Deployment* (CRC Press, 2016).

7 See, e.g., "Security Evaluation of ES&S Voting Machines and Election Management System," Adam Aviv et al., Department of Computer and Information Science, University of Pennsylvania, https://www.usenix.org/legacy/event/evt08/tech/full_papers/aviv/aviv.pdf; "EVEREST: Evaluation and Validation of Election-Related Equipment, Standards, and Testing," December 7, 2007, https://www.eac.gov/assets/1/28/EVEREST.pdf; "DEFCON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure," Matt Blaze et al., September 2017, https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf; "DEF CON 26 Voting Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure," Matt Blaze et al., September 2018, https://www.defcon.org/images/defcon-26/DEF%20CON%2026%20voting%20village%20report.pdf.

8 See *The Verifier: Polling Place Equipment in Pennsylvania—November 2018*, Verified Voting https://www.brennancenter.org/analysis/americas-voting-machines-risk-an-update#_ednref8.

9 Ben Wofford, "How to Hack an Election in 7 Minutes," *Politico*, Aug. 5, 2016, https://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144#ixzz4GTrrmQ74; "The Verifier: Polling Place Equipment in Pennsylvania, Montgomery County—November 2018," Verified Voting, https://www.verifiedvoting.org/verifier/#year/2018/state/42/county/91.

10 "Current State of Elections in Pennsylvania: Pennsylvania Department of State Election Policy Summit," Pennsylvania Department of State, April 19, 2017, http://www.dos.pa.gov/VotingElections/Documents/Election%20Policy%20Summit%20Presentations/Marian%20Schneider%20Presentation.pdf.

11 "DEFCON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure," Matt Blaze et al., September 2017, https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf.

12 "DEF CON 26 Voting Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure," Matt Blaze et al., September 2018, https://www.defcon.org/images/defcon-26/DEF%20CON%2026%20voting%20village%20report.pdf.

13 Some DRE voting systems produce event logs that can be examined to ensure that all relevant files have been collected from precinct devices and to determine that data in the election management system are correct. However, those actions will not uncover errors or interference in the tabulation software, and the inability to detect such errors could impact the outcome of an election contest.

14 Dustin Volz and Patricia Zengerle, "Inability to Audit U.S. Elections a 'National Security Concern': Homeland Chief," *Reuters*, March 21, 2018, https://www.reuters.com/article/us-usa-trump-russia-security/inability-to-audit-u-s-elections-a-*national*-security-concern-homeland-chief-idUSKBN1GX200. Secretary Nielsen has also "called on all election officials to ensure that every American votes on a verifiable and *auditable* ballot by the 2020 election." See "Secretary Kirstjen M. Nielsen Remarks to the National Election Security Summit: As Prepared for Delivery," September 10, 2018, https://www.dhs.gov/news/2018/09/10/secretary-kirstjen-m-nielsen-remarks-national-election-security-summit.

15 Testimony of Matthew Blaze, associate professor of computer and information science, University of Pennsylvania, before the U.S. House of Representatives Committee on Oversight and Government Reform Subcommittee on Information Technology and Subcommittee on Intergovernmental Affairs, Hearing on the Cybersecurity of Voting Machines, November 29, 2017, https://oversight.house.gov/wp-content/uploads/2017/11/Blaze-UPenn-Statement-Voting-Machines-11-29.pdf

16 "A Handbook for Elections Infrastructure Security," p. 19, Center for Internet Security, https://www.cisecurity.org/wp-content/uploads/2018/03/CIS-Elections-Handbook-19-March-Single-Pgs.pdf.

17 "Election Systems and Software (ES&S) Model 100," Verified Voting, https://www.verifiedvoting.org/resources/voting-equipment/ess/m100/.

18 See "The Verifier: Polling Place Equipment in Pennsylvania—November 2018," Verified Voting, https://www.verifiedvoting.org/verifier/#year/2018/state/42.

19 "Election Systems and Software (ES&S) iVotronic," Verified Voting, https://www.verifiedvoting.org/resources/voting-equipment/ess/ivotronic/.

20 "Election Systems and Software (ES&S) iVotronic," Verified Voting, https://www.verifiedvoting.org/resources/voting-equipment/ess/ivotronic/, "Security Evaluation of ES&S Voting Machines and Election Management System," Adam Aviv et al., Department of Computer and Information Science, University of Pennsylvania., p. 4, https://www.usenix.org/legacy/event/evt08/tech/full_papers/aviv/aviv.pdf.

21 William R. Cunha et al., "Election Security in Allegheny County and the Commonwealth of Pennsylvania," Heinz College of Information Systems and Public Policy, Carnegie Mellon University (May 10, 2018).

22 In fact, Professor Halderman has hacked this exact machine in a widely viewed video using compromised media used for ballot programing and other functions J. Alex Halderman, "I Hacked an Election. So Can the Russians," The New York Times, April 5, 2018, https://www.nytimes.com/2018/04/05/opinion/election-voting-machine-hacking-russians.html. Professor Halderman described to the commission similar likely attack scenarios on election management systems.

23 For purposes of this paper—and consistent with the approach of the Center for Internet Security's handbook—tallying does not entail the tabulation of votes within a specific voting machine. Rather, tallying is focused on the aggregation of votes across polling places and counties. "A Handbook for Elections Infrastructure Security," p. 22, Center for Internet Security, https://www.cisecurity.org/wp-content/uploads/2018/03/CIS-Elections-Handbook-19-March-Single-Pgs.pdf.

24 Pennsylvania counties accomplish tallying and election-night reporting in multiple ways; however, a common tactic is for polling places to provide counties with vote totals that are then tallied at the county level. Additional state guidance can be found in a document published by the Pennsylvania Department of State, setting forth pre–Election Day, Election Day, and post–Election Day procedures when an electronic voting system is to be used. "Pre-Election Day Procedures when an Electronic Voting System (EVS) Will Be Used," Pennsylvania Department of State, http://www.dos.pa.gov/VotingElections/Documents/Elections%20Division/Administration/EVS%20Pre%20During%20Post%20Election%20Day%20Procedures.pdf.

25 See, e.g., 25 Pa. Stat. Ann. § 3154.

26 William R. Cunha et al., "Election Security in Allegheny County and the Commonwealth of Pennsylvania," Heinz College of Information Systems and Public Policy, Carnegie Mellon University (May 10, 2018).

27 See, e.g., the election-night reporting results in Allegheny County for the recent midterm elections. "General Election: Unofficial Election Night Final (Includes Absentees)," Allegheny County, Pa., November 6, 2018, https://results.enr.clarityelections.com/PA/Allegheny/92253/Web02.216033/#/.

28 "2018 General Election: Unofficial Returns," Pennsylvania Department of State, https://electionreturns.pa.gov/ReportCenter/Reports.

29 "A Handbook for Elections Infrastructure Security," p. 23, Center for Internet Security, https://www.cisecurity.org/wp-content/uploads/2018/03/CIS-Elections-Handbook-19-March-Single-Pgs.pdf.

30 "The State and Local Election Cybersecurity Playbook," Harvard Kennedy School, Belfer Center for Science and International Affairs, p. 37, https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf.

31 "What Is a Man-in-the-Middle Attack?" Symantec Corp., https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html.

32 "Election Security in All 50 States: Defending America's Elections," Danielle Root et al., Center for American Progress, p. 155, https://cdn.americanprogress.org/content/uploads/2018/02/11130702/020118_ElectionSecurity-report1.pdf.

33 Ibid.; see also "Post-Election General Reconciliation Checklist," Pennsylvania Department of State, https://www.dos.pa.gov/VotingElections/OtherServicesEvents/Documents/DOS%20Post-election%20Reconciliation_November%202016.pdf.

34 See also 25 Pa. Stat. Ann. § 3154(f) ("As the returns from each election district are read, computed, and found to be correct or corrected as aforesaid, they shall be recorded on the blanks prepared for the purpose until all the returns from the various election districts which are entitled to be counted shall have been duly recorded, when they shall be added together, announced and attested by the clerks who made and computed the entries respectively and signed by the members of the county board.").

35 "Post-Election General Reconciliation Checklist," Pennsylvania Department of State, https://www.dos.pa.gov/VotingElections/OtherServicesEvents/Documents/DOS%20Post-election%20Reconciliation_November%202016.pdf.

36 "The State and Local Election Cybersecurity Playbook," Harvard Kennedy School, Belfer Center for Science and International Affairs, pp. 40–41, https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf.

37 "Voting Technology in Pennsylvania, Report of the Advisory Committee on Voting Technology," Joint State Government Commission, Table 10, http://sg.legis.state.pa.us/publications.cfm?JSPU_PUBLN_ID=463. According to the report, fifty-three of the sixty-seven Pennsylvania counties rely on vendors for one of these services: maintenance, ballot printing, ballot definition and setup, or logic and accuracy testing.

38 United States v. Netyksho, Indictment ¶¶ 73–76, No. 1:18-cr-215 (ABJ) (D.D.C. July 13, 2018), https://www.justice.gov/file/1080281/download.

39 "The State and Local Election Cybersecurity Playbook," Harvard Kennedy School, Belfer Center for Science and International Affairs, p. 35, https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf.

40 "On Election Day, Most Voters Use Electronic or Optical-Scan Ballots," Drew Desilver, Pew Research Center, http://www.pewresearch.org/fact-tank/2016/11/08/on-election-day-most-voters-use-electronic-or-optical-scan-ballots/.

41 This information was current as of November 2018. Note that a single New Jersey county (Warren County) uses DREs with paper trails.

42 Many states, including Pennsylvania, purchased new voting equipment after Congress—through the Help America Vote Act of 2002 (HAVA)—directed more than $3 billion in new funding to help states acquire new voting equipment. Most of Pennsylvania's machines were purchased around 2006 with HAVA funding.

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

44 Ibid.

45 "America's Voting Machines at Risk," Lawrence Norden and Christopher Famighetti, Brennan Center for Justice, p. 14, https://www.brennancenter.org/sites/default/files/legacy/Democracy/Paperless_Registration_FINAL.pdf.

46 The Presidential Commission on Election Administration has called this an "impending crisis in voting technology" due to "widespread wearing out of voting machines purchased a decade ago" and other concerns. "The American Voting Experience: Report and Recommendations of the Presidential Commission on Election Administration," Presidential Commission on Election Administration, p. 62, https://www.eac.gov/assets/1/6/Amer-Voting-Exper-final-draft-01-09-14-508.pdf. Risks associated with older machines include "increased failures and crashes, which can lead to long lines and lost votes," and security flaws. "America's Voting Machines at Risk," Lawrence Norden and Christopher Famighetti, Brennan Center for Justice, p. 4, https://www.brennancenter.org/sites/default/files/legacy/Democracy/Paperless_Registration_FINAL.pdf

47 "Paper Trails for All," Edgardo Cortés and Lawrence Norden, Brennan Center for Justice, http://www.brennancenter.org/blog/paper-trails-all.

48 See, e.g., "Securing the Vote: Protecting American Democracy," National Academies of Sciences, Engineering, and Medicine, Recommendation 4.11, https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy ("Elections should be conducted with human-readable paper ballots. These may be marked by hand or by machine (using a ballot-marking device); they may be counted by hand or by machine (using an optical scanner)."); Testimony of Matthew Blaze, associate professor of computer and information science, University of Pennsylvania, before the U.S. House of Representatives Committee on Oversight and Government Reform Subcommittee on Information Technology and Subcommittee on Intergovernmental Affairs, Hearing on the Cybersecurity of Voting Machines, November 29, 2017, https://oversight.house.gov/wp-content/uploads/2017/11/Blaze-UPenn-Statement-Voting-Machines-11-29.pdf ("Among currently available, HAVA-compliant voting technologies, the state of the art in this regard are precinct-counted optical scan systems."); Testimony of J. Alex Halderman, professor of computer science, University of Michigan, before the U.S. Senate Select Committee on Intelligence, June 21, 2017, https://jhalderm.com/pub/misc/ssci-voting-testimony17.pdf ("Optical scan ballots paired with risk-limiting audits provide a practical way to detect and correct vote-changing cyberattacks. They may seem low-tech, but they are a reliable, cost-effective defense."); and Testimony of Dan S. Wallach, professor, Department of Computer Science Rice Scholar, Baker Institute for Public Policy Rice University, Houston, Texas, before the House Committee on Space, Science, and Technology hearing, "Protecting the 2016 Elections from Cyber and Voting Machine Attacks," September 13, 2016, https://www.cs.rice.edu/~dwallach/pub/us-house-sst-voting-13sept2016.pdf.

49 Routine and rigorous post-election audits must still be in place to ensure the accuracy of the software tabulation of the paper records. See, e.g., "Securing the Vote: Protecting American Democracy," National Academies of Sciences, Engineering, and Medicine, Recommendation 5.5, https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy ("Each state should require a comprehensive system of post-election audits of processes and outcomes."). The commission does not recommend systems with bar codes or QR codes, as they are not human readable.

50 "Securing the Vote: Protecting American Democracy," National Academies of Sciences, Engineering, and Medicine, Recommendation 4.11, https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy.

51 Testimony of Dan S. Wallach, professor, Department of Computer Science Rice Scholar, Baker Institute for Public Policy Rice University, Houston, Texas, before the House Committee on Space, Science, and Technology hearing, "Protecting the 2016 Elections from Cyber and Voting Machine Attacks," September 13, 2016, https://www.cs.rice.edu/~dwallach/pub/us-house-sst-voting-13sept2016.pdf.

52 "Securing Elections from Foreign Interference," Lawrence Norden and Ian Vandewalker, Brennan Center for Justice, p. 11, https://www.brennancenter.org/sites/default/files/publications/Securing_Elections_From_Foreign_Interference_1.pdf.

53 Counties should be aware that some of the user interfaces found on DREs are available on ballot-marking devices. Routine and rigorous post-election audits must still be in place to ensure the accuracy of the software tabulation of the paper records. As noted above, the commission does not recommend systems with bar codes or QR codes, as they are not human readable.

54 "Joint State Government Commission, Voting Technology in Pennsylvania, Report of the Advisory Committee on Voting Technology," p. 66, http://jsg.legis.state.pa.us/publications.cfm?JSPU_PUBLN_ID=463.

55 "Department of State Tells Counties to Have New Voting Systems in Place by End of 2019," Department of State, http://www.media.pa.gov/Pages/State-Details.aspx?newsid=276. Susquehanna County was the first county to purchase new voting equipment in compliance with the Department of State directives. "First County Buys Voting Machines Under New State Standards," Penn Live, Sep. 20, 2018, https://www.pennlive.com/politics/index.ssf/2018/09/first_county_buys_voting_machi.html. Montgomery County also recently announced the purchase of a new voting system. "Montgomery County Commissioners Select New Voting System," Montgomery County Board of Commissioners, https://www.montcopa.org/ArchiveCenter/ViewFile/Item/4669.

56 "Wolf Administration Directs That New Voting Systems in the Commonwealth Provide Paper Record," Department of State, http://www.media.pa.gov/Pages/State-Details.aspx?newsid=261.

57 Stein v. Cortes, Settlement Agreement ¶¶ 2–4, No. 2:16-cv-6287 (PD), ECF No. 108, (E.D. Pa. Nov. 28, 2018).

58 "A Gentle Introduction to Risk-Limiting Audits," Mark Lindeman and Philip B. Stark, IEE Security and Privacy: Special Issue on Electronic Voting, p. 1, https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

59 According to Disability Rights Pennsylvania, HAVA "requires voting systems [to be] accessible for people with disabilities, including the blind and visually impaired, in a manner that provides the same opportunity for access and participation as other voters." "Fact Sheet: Voting by People with Disabilities Ensuring Participation for All Citizens," Disability Rights Pennsylvania, p. 3, https://www.disabilityrightspa.org/wp-content/uploads/2018/03/VotingByPWDFactsheetFEB2018.pdf.

60 Conversation with Michelle Bishop, voting rights specialist, National Disability Rights Network, June 7, 2018.

61 DRE machines also do not allow for any voters to independently verify their votes. However, a tenet of HAVA is *equal* access.

62 See, e.g., "Fact Sheet: Voting by People with Disabilities Ensuring Participation for All Citizens," Disability Rights Pennsylvania, p. 3, https://www.disabilityrightspa.org/wp-content/uploads/2018/03/VotingByPWDFactsheetFEB2018.pdf; "Disability Voting Issues—Access, Assistance, and Accommodations," Disability Rights Pennsylvania, https://www.disabilityrightspa.org/wp-content/uploads/2018/03/DisabilityVotingIssuesAccessAssistanceAccommodationsFEB2018.pdf.

63 See, e.g., "Fact Sheet: Voting by People with Disabilities Ensuring Participation for All Citizens," Disability Rights Pennsylvania, p. 3, https://www.disabilityrightspa.org/wp-content/uploads/2018/03/VotingByPWDFactsheetFEB2018.pdf; "Disability Voting Issues—Access, Assistance, and Accommodations," Disability Rights Pennsylvania, https://www.disabilityrightspa.org/wp-content/uploads/2018/03/DisabilityVotingIssuesAccessAssistanceAccommodationsFEB2018.pdf.

64 Cat Zakrzewski, "The Cybersecurity 202: At Least Six States Still Might Not Have Paper Ballot Backups in 2010," *Washington Post*, Nov. 21, 2018, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/11/21/the-cybersecurity-202-at-least-six-states-still-might-not-have-paper-ballot-backups-in-2020/5bf4b7aa1b326b60d127ffe5/?utm_term=.6b0d2bac55cc.

65 See "Directive Concerning the Conduct of Electronic Voting System Examinations by the Commonwealth of Pennsylvania Issued by the Secretary of the Commonwealth, https://www.dos.pa.gov/VotingElections/Documents/Voting%20Systems/Directives/Directive%20to%20Vendors%20v06122018.pdf.

66 "Electronic Voting Systems," Pennsylvania Department of State, https://www.dos.pa.gov/VotingElections/OtherServicesEvents/Pages/Voting-Systems.aspx#VihhuclRqPI.

67 Letter from Kathryn Boockvar, senior advisor to the governor on election modernization, Pennsylvania Department of State, dated August 7, 2018 (on file with commission).

68 "Q&A. What Will Have to Be Done to Upgrade PA's Voting Systems?" *PennLive*, April 13, 2018, http://www.pennlive.com/news/2018/04/qa_what_will_have_to_be_done_t.html.

69 "Counties React to DOS Acting Secretary Torres' Voting Equipment Directive," Douglas E. Hill, County Commissioners Association of Pennsylvania, https://www.pacounties.org/Media/Lists/NewsRelease/customDisplay.aspx?ID=48&RootFolder=%2FMedia%2FLists%2FNewsRelease&Source=https%3A%2F%2Fwww%2Epacounties%2Eorg%2FMedia%2FPages%2Fdefault%2Easpx. A 2018 analysis by the Brennan Center and Verified Voting found that the cost for Pennsylvania to replace all of its DRE voting machines without voter-verifiable paper audit trails would be $50.4 million to $79.1 million. However, the estimate is based on equipment, not on maintenance, software licensing, or training. See "Proposed Election Infrastructure Spending," Brennan Center for Justice, https://www.brennancenter.org/analysis/proposed-election-infrastructure-spending.

70 Sarah Breitenbach, "Aging Voting Machines Cost Local, State Governments," *Pew Stateline*, March 2, 2016, http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2016/03/02/aging-voting-machines-cost-local-state-governments.

71 "Are Voter-verified Paper Ballots Cost Effective?" Verified Voting, https://www.verifiedvoting.org/downloads/Newvvpbcosts.pdf.

72 "Federal Funds for Election Security: Will They Cover the Costs of Voter Marked Paper Ballots?," Brennan Center for Justice, n.1, http://www.brennancenter.org/analysis/federal-funds-election-security-will-they-cover-costs-voter-marked-paper-ballots#_ftn1.

73 For sample acquisition cost comparisons of DREs versus optical scans for selected states, see "Are Voter-Verified Paper Ballots Cost Effective?" Verified Voting, https://www.verifiedvoting.org/downloads/Newvvpbcosts.pdf.

74 "Proposed Election Infrastructure Spending," Brennan Center for Justice, https://www.brennancenter.org/analysis/proposed-election-infrastructure-spending.

75 "Q&A. What Will Have To Be Done to Upgrade PA's Voting Systems," *PennLive*, April 13, 2018, http://www.pennlive.com/news/2018/04/qa_what_will_have_to_be_done_t.html.

76 For a brief review of how other states have funded the purchase of new voting machines, see the National Conference of State Legislatures, Funding Elections Technology, January 11, 2018. Last visited May 30, 2018. http://www.ncsl.org/research/elections-and-campaigns/funding-election-technology.aspx.

77 Pa. Const. Art. 8, §7(a)(4) ("Debt may be incurred without the approval of the electors for capital projects specifically itemized in a capital budget, if such debt will not cause the amount of all net debt outstanding to exceed one and three-quarters times the average of the annual tax revenues deposited in the previous five fiscal years as certified by the Auditor General.").

78 72 Pa. Stat. Ann. § 3919.302.

79 "Guidance on Electronic Voting System Preparation and Security," Pennsylvania Department of State, https://www.dos.pa.gov/VotingElections/OtherServicesEvents/Documents/DOS%20Guidance%20Electronic%20Voting%20System%20Security%2009232016.pdf.

80 "A Handbook for Elections Infrastructure Security," pp. 38–59, Center for Internet Security, https://www.cisecurity.org/wp-content/uploads/2018/03/CIS-Elections-Handbook-19-March-Single-Pgs.pdf.

81 Project Shield, https://projectshield.withgoogle.com/public/.

82 Athenian Project, https://www.cloudflare.com/athenian-project/.

83 "Post-Election General Reconciliation Checklist," Pennsylvania Department of State, https://www.dos.pa.gov/VotingElections/OtherServicesEvents/Documents/DOS%20Post-election%20Reconciliation_November%202016.pdf.

84 For example, a California law requires such reporting by vendors within 30 days of a vendor learning of such an issue. See Cal. Elec. Code § 19215(a).

85 "Russia/Cybersecurity," National Security Agency, https://www.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing.html#document/p1

86 Ibid.

87 United States v. Netyksho, Indictment ¶ 76, No. 1:18-cr-215 (ABJ) (D.D.C. July 13, 2018), https://www.justice.gov/file/1080281/download.

88 Ibid. ¶ 75.

89 Likhitha Butchireddygari, "Many County Election Officials Still Lack Cybersecurity Training," NBC News, August 23, 2017, https://www.nbcnews.com/politics/national-security/voting-prep-n790256.

90 Allegheny County did, however, report having received training from federal officials, and Bucks County reported that personnel had received cybersecurity training from county information technology personnel.

91 Likhitha Butchireddygari, "Many County Election Officials Still Lack Cybersecurity Training," NBC News, August 23, 2017, https://www.nbcnews.com/politics/national-security/voting-prep-n790256.

92 Ibid.

93 Telephone interview with Kathryn Boockvar, senior advisor to the governor on election modernization, Pennsylvania Department of State; Jonathan Marks, commissioner, Bureau of Commissions, Elections, and Legislation, Pennsylvania Department of State; John MacMillan, Pennsylvania chief information officer; and Erik Avakian, Pennsylvania chief information security officer, September 20, 2018.

94 "Federal Virtual Training Environment (FedVTE)," Department of Homeland Security, National Institute for Cybersecurity Careers and Studies, https://niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte.

95 "DHS Election Infrastructure Security Resource Guide," Department of Homeland Security, pp. 17–18, https://www.dhs.gov/sites/default/files/publications/DHS%20Election%20Infrastructure%20Security%20Resource%20Guide%20April%202018.pdf.

96 This report includes a more thorough discussion of contingency planning in the section on "Recovery and Resilience."

97 "Albert," Center for Internet Security, https://www.cisecurity.org/services/albert/.

98 "Amidst Reports of Russian Hacking, Governor Cuomo Unveils Comprehensive Initiative to Strengthen State's Election Cyber Security Infrastructure and Protect against Foreign Interference," New York Governor Andrew M. Cuomo, https://www.governor.ny.gov/news/amidst-reports-russian-election-hacking-governor-cuomo-unveils-comprehensive-initiative.

99 "Russian Targeting of Election Infrastructure during the 2016 Election: Summary of Initial Findings and Recommendations," U.S. Senate Intelligence Committee, https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf.

100 Ibid.

101 Ibid.

102 "DHS State Notification and State Public Statements," National Association of Secretaries of State, https://www.nass.org/sites/default/files/chart-dhs-state-notifications-public-statements092917.pdf.

103 "Russians Targeted Pennsylvania Election System," Associated Press, PennLive, Sept. 22, 2017, https://www.pennlive.com/politics/index.ssf/2017/09/russians_targeted_pennsylvania.html.

104 "Russian Targeting of Election Infrastructure during the 2016 Election: Summary of Initial Findings and Recommendations," U.S. Senate Intelligence Committee, https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf.

105 United States v. Netyksho, Indictment ¶ 72, No. 1:18-cr-215 (ABJ) (D.D.C. July 13, 2018), https://www.justice.gov/file/1080281/download.

106 Ibid. ¶ 73.

107 Pa. Act of Jan. 31, 2002, Pub. L. 18, No. 3, http://www.legis.state.pa.us/cfdocs/legis/li/uconsCheck.cfm?yr=2002&sessInd=0&act=3.

108 "A Handbook for Elections Infrastructure Security," p. 13, Center for Internet Security, https://www.cisecurity.org/wp-content/uploads/2018/03/CIS-Elections-Handbook-19-March-Single-Pgs.pdf.

109 "The Administration of Voter Registration in Pennsylvania: 2016 Report to the General Assembly," Secretary of the Commonwealth, Pennsylvania Department of State, p. 14, http://www.dos.pa.gov/VotingElections/OtherServicesEvents/Documents/2016%20Annual%20Report%2006302017_final.pdf

110 "Voter Registration in a Digital Age," Christopher Ponoroff, Brennan Center for Justice, p. 17, https://www.brennancenter.org/sites/default/files/legacy/Democracy/Paperless_Registration_FINAL.pdf; "Voter Registration in a Digital Age: Pennsylvania," Brennan Center for Justice, https://www.brennancenter.org/sites/default/files/legacy/Democracy/Paperless%20Report%20Appendix_Final%20(Pennsylvania).pdf

111 "The Administration of Voter Registration in Pennsylvania: 2016 Report to the General Assembly," Secretary of the Commonwealth, Pennsylvania Department of State, p. 14, http://www.dos.pa.gov/VotingElections/OtherServicesEvents/Documents/2016%20Annual%20Report%2006302017_final.pdf

112 These methods are in addition to those available to military and overseas voters. See "Information for Military and Overseas Voters," Pennsylvania Department of State, Votes PA, http://www.votespa.com/Voting-in-PA/Pages/Military-and-Overseas-Voters.aspx

113 "Register to Vote," Pennsylvania Department of State, Votes PA, http://www.votespa.com/Register-to-Vote/Pages/default.aspx; "How and Where to Register to Vote," Pennsylvania Department of State, Votes PA, http://www.votespa.com/Register-to-Vote/Pages/How-to-Register-to-Vote.aspx.

114 "How and Where to Register to Vote," Pennsylvania Department of State, Votes PA, http://www.votespa.com/Register-to-Vote/Pages/How-to-Register-to-Vote.aspx. Completed applications received at PennDOT locations are transmitted electronically to the Department of State and placed into the county election officials' workflow via SURE. "The Administration of Voter Registration in Pennsylvania: 2016 Report to the General Assembly," Secretary of the Commonwealth, Pennsylvania Department of State, p. 11, http://www.dos.pa.gov/VotingElections/OtherServicesEvents/Documents/2016%20Annual%20Report%2006302017_final.pdf.

115 "Voter Registration Application," Pennsylvania Department of State, https://www.pavoterservices.pa.gov/pages/VoterRegistrationApplication.aspx

116 "A Handbook for Elections Infrastructure Security," p. 16, Center for Internet Security, https://www.cisecurity.org/wp-content/uploads/2018/03/CIS-Elections-Handbook-19-March-Single-Pgs.pdf.

117 See 25 Pa. Stat. and Cons. Stat. Ann. § 1401(c) ("After a commission is connected to the SURE system, the general register of the commission shall consist of the registration information contained on the SURE system as maintained by the commission."); § 1402(b)(2) ("After a commission is connected to the SURE system, each commission shall create from its general register a computer list to be used as the district register.").

118 25 Pa. Stat. Ann. § 3050; see also William R. Cunha et al., "Election Security in Allegheny County and the Commonwealth of Pennsylvania," Heinz College of Information Systems and Public Policy, Carnegie Mellon University, p. 4.

119 William R. Cunha et al., "Election Security in Allegheny County and the Commonwealth of Pennsylvania," Heinz College of Information Systems and Public Policy, Carnegie Mellon University, p. 4; "A Look at How—and How Many—States Adopt Electronic Poll Books," Pew Charitable Trusts, http://www.pewtrusts.org/en/research-and-analysis/data-visualizations/2017/a-look-at-how-and-how-many-states-adopt-electronic-poll-books

120 Electronic pollbooks are subject to a test protocol promulgated by the Department of State. See "EPB Test Protocol," Pennsylvania Department of State, https://www.eac.gov/assets/1/28/Pennsylvania%20EPB%20Test%20Protocol.pdf

121 "Pennsylvania Voting System and Electronic Poll Book Report," Pennsylvania Department of State, https://www.dos.pa.gov/VotingElections/Documents/Voting%20Systems/Voting%20System%20Status%20Report/Voting%20System%20Status%20Report_October%202018.pdf

122 "The State of Voting 2018," Wendy Weiser and Max Feldman, Brennan Center for Justice, p. 4, https://www.brennancenter.org/sites/default/files/publications/2018_06_StateOfVoting_v5%20%281%29.pdf.

123 Ibid.

124 "Advertisement Information," PA e-Marketplace, Supplier Service Center, Bureau of Procurement, http://www.emarketplace.state.pa.us/Solicitations.aspx?SID=6100044816-SE

125 "Auditor General DePasquale Expands Scope of Voting Security Audit Outreach in Wake of Latest Indictments of Russian Hackers," Pennsylvania Department of the Auditor General, https://www.paauditor.gov/press-releases/auditor-general-depasquale-expands-scope-of-voting-security-audit-outreach-in-wake-of-latest-indictments-of-russian-hackers; "Auditor General DePasquale Launches Audit to Safeguard Voting Security," Pennsylvania Department of the Auditor General, http://www.paauditor.gov/press-releases/auditor-general-depasquale-launches-audit-to-safeguard-voting-security.

126 William R. Cunha et al., "Election Security in Allegheny County and the Commonwealth of Pennsylvania," Heinz College of Information Systems and Public Policy, Carnegie Mellon University (May 10, 2018).

127 Ibid., 5.

128 Ibid., 6.

129 "PA Full Voter Export," Pennsylvania Department of State, https://www.pavoterservices.pa.gov/pages/purchasepafullvoterexport.aspx.

130 "Find Your Polling Place," Pennsylvania Department of State, https://www.pavoterservices.pa.gov/pages/pollingplaceinfo.aspx.

131 See, e.g., Zaid Shoorbajee, "Researcher Finds Trove of Political Fundraising, Old Voter Data on Open Internet," *CyberScoop*, October 24, 2018, https://www.cyberscoop.com/rice-consulting-nas-exposed-voter-data/

132 William R. Cunha et al., "Election Security in Allegheny County and the Commonwealth of Pennsylvania," Heinz College of Information Systems and Public Policy, Carnegie Mellon University (May 10, 2018), p. 6.

133 "Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections," Latanya Sweeney et al., https://techscience.org/a/2017090601/

134 Ibid., 95.

135 Shaun Waterman, "Election Officials Criticize Harvard Study of Voter Registration Vulnerabilities," *CyberScoop* September 6, 2017, https://www.cyberscoop.com/harvard-study-online-voter-registration-vulnerabilities-election-officials-pushback/.

136 " Security Tip (ST04-015): Understanding Denial-of-Service Attacks," U.S. Department of Homeland Security, https://www.us-cert.gov/ncas/tips/ST04-015.

137 "The State and Local Election Cybersecurity Playbook," Harvard Kennedy School, Belfer Center for Science and International Affairs, p. 28, https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf.

138 According to Commonwealth officials, the Department of State is already considering implementation of this added level of encryption.

139 "DHS Election Infrastructure Security Funding Consideration," U.S. Department of Homeland Security, Appendix: Vendor Selection Considerations, https://www.dhs.gov/sites/default/files/publications/Election%20Infrastructure%20Security%20Funding%20Considerations%20Final.pdf.

140 "A Handbook for Elections Infrastructure Security," p. 64–68, Center for Internet Security, https://www.cisecurity.org/wp-content/uploads/2018/03/CIS-Elections-Handbook-19-March-Single-Pgs.pdf.

141 Eric Geller, "Russia Fears Have Election Vendors Feeling the Heat," *Politico*, February 24, 2018, https://www.politico.com/story/2018/02/24/elections-vendors-russia-423435.

142 See, e.g., "The State and Local Election Cybersecurity Playbook," Harvard Kennedy School, Belfer Center for Science and International Affairs, Appendix 1 (Vendor Selection and Management), https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf

143 Dustin Volz and Patricia Zengerle, "Inability to Audit U.S. Elections a 'National Security Concern': Homeland Chief," *Reuters*, March 21, 2018, https://www.reuters.com/article/us-usa-trump-russia-security/inability-to-audit-u-s-elections-a-national-security-concern-homeland-chief-idUSKBN1GX200.

144 "Secretary Kirstjen M. Nielsen, Remarks to the National Election Security Summit: As Prepared for Delivery," September 10, 2018, https://www.dhs.gov/news/2018/09/10/secretary-kirstjen-m-nielsen-remarks-national-election-security-summit.

145 Pa. Cons. Stat. Tit. 25 Sec. 3031.17.

146 See, e.g., "Securing the Vote: Protecting American Democracy," National Academies of Sciences, Engineering, and Medicine, Recommendations 4.11–13, 5.5–10, https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy; Testimony of J. Alex Halderman, professor of computer science, University of Michigan, before the U.S. Senate Select Committee on Intelligence, June 21, 2017, https://jhalderm.com/pub/misc/ssci-voting-testimony17.pdf; Testimony of Matthew Blaze, associate professor of computer and information science, University of Pennsylvania, before the U.S. House of Representatives Committee on Oversight and Government Reform Subcommittee on Information Technology and Subcommittee on Intergovernmental Affairs, Hearing on the Cybersecurity of Voting Machines, November 29, 2017, https://oversight.house.gov/wp-content/uploads/2017/11/Blaze-UPenn-Statement-Voting-Machines-11-29.pdf; Testimony of Dan S. Wallach, professor, Department of Computer Science Rice Scholar, Baker Institute for Public Policy Rice University, Houston, Texas, before the House Committee on Space, Science, and Technology hearing, "Protecting the 2016 Elections from Cyber and Voting Machine Attacks," September 13, 2016, https://www.cs.rice.edu/~dwallach/pub/us-house-sst-voting-13sept2016.pdf; "Securing the Nation's Voting Machines," Brennan Center for Justice, Common Cause, National Election Defense Coalition, VerifiedVoting, https://www.brennancenter.org/publication/securing-nations-voting-machines.

147 Testimony of Matthew Blaze, associate professor of computer and information science, University of Pennsylvania, before the U.S. House of Representatives Committee on Oversight and Government Reform Subcommittee on Information Technology and Subcommittee on Intergovernmental Affairs, Hearing on the Cybersecurity of Voting Machines, November 29, 2017, https://oversight.house.gov/wp-content/uploads/2017/11/Blaze-UPenn-Statement-Voting-Machines-11-29.pdf.

148 "A Gentle Introduction to Risk-Limiting Audits," Mark Lindeman and Philip B. Stark, IEE Security and Privacy: Special Issue on Electronic Voting, https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.; "A Smart and Effective Way to Safeguard Elections," Christopher Deluzio, Brennan Center for Justice, https://www.brennancenter.org/blog/smart-and-effective-way-safeguard-elections.

149 "A Gentle Introduction to Risk-Limiting Audits," Mark Lindeman and Philip B. Stark, IEE Security and Privacy: Special Issue on Electronic Voting, p. 1, https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

150 "A Gentle Introduction to Risk-Limiting Audits," Mark Lindeman and Philip B. Stark, IEE Security and Privacy: Special Issue on Electronic Voting, p. 1, https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

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

152 Eric Geller, "Colorado to Require Advanced Post-Election Audits," Politico, July 17, 2017, https://www.politico.com/story/2017/07/17/colorado-post-election-audits-cybersecurity-240631.

153 "Risk-Limiting Audits—Practical Application," Jerome Lovato, U.S. Election Assistance Commission, https://www.eac.gov/assets/1/6/Risk-Limiting_Audits_-_Practical_Application_Jerome_Lovato.pdf. Almost all Colorado counties now have voting systems that support the most efficient risk-limiting audits, ballot-level comparison audits.

154 "Post Election Audits," Verified Voting, https://www.verifiedvoting.org/resources/post-election-audits/.

155 "Risk-Limiting Audits," Verified Voting, https://www.verifiedvoting.org/resources/post-election-audits/risk-limiting-audits/.

156 "Election Rules, 8 CCR 1505-1, Rule 25, Post-Election Audit," Colorado Department of State, http://www.sos.state.co.us/pubs/rule_making/CurrentRules/8CCR1505-1/Rule25.pdf.

157 Eric Geller, "Colorado to Require Advanced Post-Election Audits," *Politico*, July 17, 2017, https://www.politico.com/story/2017/07/17/colorado-post-election-audits-cybersecurity-240631.

158 "The Colorado Risk-Limiting Audit Project (CORLA)," http://bcn.boulder.co.us/~neal/elections/corla/.

159 RI Gen L Sec. 17-19-37.4 (2017). Virginia also has a statutory requirement for risk-limiting audits. See "Virginia Acts of Assembly—2017 Session: Chapter 367, http://lis.virginia.gov/cgi-bin/legp604.exe?171+ful+CHAP0367+pdf.

160 Stein v. Cortes, Settlement Agreement ¶ 5, No. 2:16-cv-6287 (PD), ECF No. 108, (E.D. Pa. Nov. 28, 2018).

161 Ibid., ¶¶ 5-6.

162 Ibid., ¶ 8.

163 Pa. Cons. Stat. Tit. 25 Sec. 3031.17.

164 "Russian Targeting of Election Infrastructure during the 2016 Election: Summary of Initial Findings and Recommendations," U.S. Senate Intelligence Committee, https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf; see also "State Laws and Practices for the Emergency Management of Elections," National Association of Secretaries of State, https://www.nass.org/sites/default/files/Election%20Cybersecurity/report-NASS-emergency-preparedness-elections-apr2017.pdf.

165 "America's Voting Machines at Risk," Lawrence Norden and Christopher Famighetti, Brennan Center for Justice, p. 30, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

166 "Cyber Incident Response Best Practices," U.S. Election Assistance Commission, https://www.eac.gov/assets/1/6/Incident-Response_best-practices.pdf.

167 "State and County Election Staff Participate in National Cyber Training Exercise," Pennsylvania Department of State, https://www.media.pa.gov/Pages/State-Details.aspx?newsid=299.

168 "Pennsylvania State and County Officials Train for Election Day Preparedness," PR Newswire, https://www.prnewswire.com/news-releases/pennsylvania-state-and-county-officials-train-for-election-day-preparedness-300719602.html.

169 Robust, statistically sound post-election audits are, as discussed elsewhere in this report, a necessary component of broader recovery and resilience planning, and the commission's recommended improvements to the Commonwealth's varied election management systems should also bolster the readiness of those systems.

170 "The State and Local Election Cybersecurity Playbook," Harvard Kennedy School, Belfer Center for Science and International Affairs, p. 61, https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf.

171 Ibid., 14.

172 "Better Safe Than Sorry: How Election Officials Can Plan Ahead to Protect the Vote in the Face of a Cyberattack," Edgardo Cortés et al., Brennan Center for Justice, p. 5, https://www.brennancenter.org/sites/default/files/publications/08.15.18_Better_Safe_Than_Sorry.pdf.

173 Telephone interview with Kathryn Boockvar, senior advisor to the governor on election modernization, Pennsylvania Department of State; Jonathan Marks, commissioner, Bureau of Commissions, Elections, and Legislation, Pennsylvania Department of State; John MacMillan, Pennsylvania chief information officer; and Erik Avakian, Pennsylvania chief information security officer, September 20, 2018.

174 "Counting Votes 2012: A State by State Look at Voting Technology Preparedness," Pamela Smith, Michelle Mulder, Susannah Goodman, p. 4, http://countingvotes.org/sites/default/files/CountingVotes2012_Final_August2012.pdf.

175 "America's Voting Machines at Risk," Lawrence Norden and Christopher Famighetti, Brennan Center for Justice, p. 30, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

176 25 Pa. Stat. Ann. § 3031.20(b).

177 "Directive Concerning the Use, Implementation, and Operation of Electronic Voting Systems by the County Boards of Elections" Pennsylvania Department of State, p. 3, https://www.dos.pa.gov/VotingElections/Documents/Elections%20Division/Administration/directive%20concerning%20the%20use.pdf. Officials established this 50% requirement as a result of a court ruling. NAACP v. Cortes, 591 F. Supp. 2d 757, 767 (E.D. Pa. 2008) (granting preliminary injunction), No. 08-5048 (E.D. Pa. Jan. 29, 2009) (granting permanent injunction), http://moritzlaw.osu.edu/electionlaw/litigation/documents/Cortes-Order-1-28-09.pdf.

178 "Directive Concerning the Use, Implementation, and Operation of Electronic Voting Systems by the County Boards of Elections" Pennsylvania Department of State, p. 3, https://www.dos.pa.gov/VotingElections/Documents/Elections%20Division/Administration/directive%20concerning%20the%20use.pdf.

179 "Emergency Paper Ballots," Pennsylvania Department of State, p. 1, https://www.dos.pa.gov/VotingElections/Documents/Elections%20Division/Administration/Use%20of%20emergency_paper_ballots.pdf.

180 Ibid.

181 25 Pa. Stat. Ann. § 2967 (requiring "for each election district in which a primary is to be held, one book of fifty official ballots of each party for every forty-five registered and enrolled electors of such party and fraction thereof, appearing upon the district register, and shall provide for each election district in which an election is to be held one book of fifty official ballots for every forty-five registered electors and fraction thereof appearing upon the district register").

182 Ibid.

183 "Better Safe Than Sorry: How Election Officials Can Plan Ahead to Protect the Vote in the Face of a Cyberattack," Edgardo Cortés et al., Brennan Center for Justice, p. 3, https://www.brennancenter.org/sites/default/files/publications/08.15.18_Better_Safe_Than_Sorry.pdf.

184 25 Pa. Cons. Stat. § 3031.14; see also "Election Security in All 50 States: Defending America's Elections," Danielle Root et al., Center for American Progress, p. 155, https://cdn.americanprogress.org/content/uploads/2018/02/21105338/020118_ElectionSecurity-report11.pdf.

185 "Poll Worker Training," Pennsylvania Department of State, https://www.votespa.com/Resources/Pages/Poll-Worker-Training.aspx.

186 "Poll Worker Training, Training to Assist Voters with Disabilities," Pennsylvania Department of State, http://pacast.com/players/cmsplayer.asp?video_filename=8747_State_ElectionDisability.m4v.

187 See, e.g., "Pollworkers Needed," Berks County, http://www.co.berks.pa.us/Dept/Elections/Pages/Pollworkers%20Needed.aspx ("Training is mandatory for new Election Officers and a refresher course for returning pollworkers is offered before each election. Election Officers should expect to spend at least two hours in an in-depth and hands-on training session. Election Officers receive additional compensation for attending a training class."); "Montgomery County PA Poll Worker Training Schedule," Montgomery County, https://www.montcopa.org/DocumentCenter/View/21912/2018-GE-Poll-Worker-Training-Schedule (listing training sessions); "Elections: Poll Workers," Northampton County, https://www.northamptoncounty.org/CTYADMN/ELECTNS/Pages/PollWorkers.aspx ("All new Poll Workers are required to attend training provided [by] the voter registration office."); "Election Board Training: 2018 Primary Election," City of Philadelphia City Commissioners, https://files.philadelphiavotes.com/election-workers/Election_Board_Training.pdf. (training presentation).

188 "Test Protocol for Examination of Election Services Online Electronic Pollbook," Pennsylvania Department of State, https://www.dos.pa.gov/VotingElections/Documents/Voting%20Systems/Know%20iNK%20Poll%20Pad/Test%20Protocol.pdf.

189 "Pennsylvania Voting System and Electronic Poll Book Report," Pennsylvania Department of State, https://www.dos.pa.gov/VotingElections/Documents/Voting%20Systems/Voting%20System%20Status%20Report/Voting%20System%20Status%20Report_Jun%202018v1.pdf.

190 See, e.g., "Results of Votec Electronic Poll Book VoteSafe (version PA-Cert) Demonstration," Pennsylvania Department of State, https://www.dos.pa.gov/VotingElections/Documents/Voting%20Systems/VoteSafe%20EPB/VOTEC%20VoteSafe%20EPB%20Secretary%27s%20report%202017.pdf.

191 "Poll Worker Training, Voter Sign-In," Pennsylvania Department of State, https://www.votespa.com/Resources/Pages/Poll-Worker-Training.aspx.

192 "A Look at How—and How Many—States Adopt Electronic Poll Books," Pew Charitable Trusts, http://www.pewtrusts.org/en/research-and-analysis/data-visualizations/2017/a-look-at-how-and-how-many-states-adopt-electronic-poll-books ("Backup EPBs available on Election Day" in Pennsylvania, under "Processing and Security" menu); see also "Election Security in All 50 States," Danielle Root et al., Center for American Progress, p. 154, https://cdn.americanprogress.org/content/uploads/2018/02/21105338/020118_ElectionSecurity-report11.pdf ("Paper voter registration lists are available at polling places that use electronic poll books on Election Day.").

193 "Better Safe Than Sorry: How Election Officials Can Plan Ahead to Protect the Vote in the Face of a Cyberattack," Edgardo Cortés et al., Brennan Center for Justice, p. 2, https://www.brennancenter.org/sites/default/files/publications/08.15.18_Better_Safe_Than_Sorry.pdf.

194 Pam Fessler, "Russian Cyberattack Targeted Elections Vendor Tied to Voting Day Disruptions," NPR, August 10, 2017, https://www.npr.org/2017/08/10/542634370/russian-cyberattack-targeted-elections-vendor-tied-to-voting-day-disruptions.

195 "Better Safe Than Sorry: How Election Officials Can Plan Ahead to Protect the Vote in the Face of a Cyberattack," at 2, Edgardo Cortés et al., Brennan Center for Justice, https://www.brennancenter.org/sites/default/files/publications/08.15.18_Better_Safe_Than_Sorry.pdf.

196 "Procedures to Assure Compliance with Provisional Balloting under the Help America Vote Act of 2002 and the Pennsylvania Election Code," Pennsylvania Department of State, pp. 1–2, https://www.dos.pa.gov/VotingElections/Documents/Elections%20Division/Administration/provisional_balloting_procedures.pdf.

197 "Provisional Ballot Guidance Summary," Pennsylvania Department of State, https://www.dos.pa.gov/VotingElections/OtherServicesEvents/Documents/DOS%20Provisional%20Ballot%20Guidance%20082015.pdf.

198 As an example, the Pennsylvania Election Code states that "an individual who claims to be properly registered and eligible to vote at the election district but whose name does not appear on the district register and whose registration cannot be determined by the inspectors of election or the county election board shall be permitted to cast a provisional ballot." 25 Pa. Stat. Ann. § 3050(a.4)(1). And federal law requires that a provisional ballot be provided to an individual who declares that they are "a registered voter in the jurisdiction in which the individual desires to vote and that the individual is eligible to vote in an election for Federal office, but the name of the individual does not appear on the official list of eligible voters for the polling place or an election official asserts that the individual is not eligible to vote." 52 U.S.C.A. § 21082(a).

199 "Procedures to Assure Compliance with Provisional Balloting under the Help America Vote Act of 2002 and the Pennsylvania Election Code," Pennsylvania Department of State, p. 2, https://www.dos.pa.gov/VotingElections/Documents/Elections%20Division/Administration/provisional_balloting_procedures.pdf.

200 "Checklist for Securing Voter Registration Data," U.S. Election Assistance Commission, https://www.eac.gov/documents/2017/10/23/checklist-for-securing-voter-registration-data/.

201 "Election Security in All 50 States: Defending America's Elections," p. 154, Danielle Root et al., Center for American Progress, https://cdn.americanprogress.org/content/uploads/2018/02/21105338/020118_ElectionSecurity-report11.pdf.

202 Testimony of Noah Praetz, director of elections, Office of Cook County Clerk, before the U.S. Senate Rules and Administration Committee, June 20, 2018, https://www.rules.senate.gov/imo/media/doc/Written%20Testimony%20of%20Noah%20Praetz_US%20Senate%20Rules%20and%20Admin_June%2020_V2.pdf.

203 "Better Safe Than Sorry: How Election Officials Can Plan Ahead to Protect the Vote in the Face of a Cyberattack," Edgardo Cortés et al., Brennan Center for Justice, p. 4, https://www.brennancenter.org/sites/default/files/publications/08.15.18_Better_Safe_Than_Sorry.pdf.

204 "Find Your Voter Registration Status," Pennsylvania Department of State, https://www.payoterservices.pa.gov/pages/voterregistrationstatus.aspx.

205 "Better Safe Than Sorry: How Election Officials Can Plan Ahead to Protect the Vote in the Face of a Cyberattack," Edgardo Cortés et al., Brennan Center for Justice, p. 5, https://www.brennancenter.org/sites/default/files/publications/08.15.18_Better_Safe_Than_Sorry.pdf.

206 "Cyber Incident Response Best Practices," U.S. Election Assistance Commission, https://www.eac.gov/assets/1/6/Incident-Response_best-practices.pdf.

207 Although the document is short (three pages), each bullet corresponding to a topic for planning is titled after a recommendation from National Institute of Standards and Technology Special Publication (SP) 800-61 Revision 2 *Computer Security Incident Handling Guide*; thus, officials can glean more detail there.

208 "Incident Handling Overview for Election Officials," U.S. Department of Homeland Security, https://www.dhs.gov/sites/default/files/publications/Incident%20Handling%20Elections%20Final%20508.pdf.

209 "Election Cyber Incident Communications Plan Template," Harvard Kennedy School, Belfer Center for Science and International Affairs, https://www.belfercenter.org/sites/default/files/files/publication/CommunicationsTemplate.pdf.

210 "Election Cyber Incident Communications Coordination Guide," Harvard Kennedy School, Belfer Center for Science and International Affairs, https://www.belfercenter.org/sites/default/files/files/publication/CommunicationsGuide.pdf.

211 "EI-ISAC Members," Center for Internet Security, https://www.cisecurity.org/ei-isac/partners-ei-isac/.

212 " Cyber Incident Checklist: Elections Infrastructure ISAC," Center for Internet Security, https://www.cisecurity.org/wp-content/uploads/2018/05/EI-ISAC-Checklist-Final.pdf.

213 "Governor Wolf Announces Interagency Workgroup to Strengthen Security of Pennsylvania Votes," Governor Tom Wolf, https://www.governor.pa.gov/governor-wolf-announces-interagency-workgroup-strengthen-security-pennsylvania-votes/.

214 *In re Gen. Election-1985*, 531 A.2d 836, 839 (Pa. Commw. Ct. 1987).

215 Id.

216 Michael T. Morley, *Election Emergencies: Voting in the Wake of Natural Disasters and Terrorist Attacks*, 67 *Emory Law Journal* 545 (2018).

217 Ibid., 615.

218 "Report of the Task Force on Emergency Preparedness for Elections," National Association of Secretaries of State, https://www.nass.org/sites/default/files/Election%20Cybersecurity/report-NASS-emergency-preparedness-elections-apr2017.pdf. Examples of other states' statutes are also available in a Congressional Research Service report. See "State Election Laws: Overview of Statutes Regarding Emergency Election Postponement within the State," Congressional Research Service, https://fas.org/sgp/crs/RS21942.pdf.

219 "Emergency Paper Ballots," Pennsylvania Department of State, p. 1, https://www.dos.pa.gov/VotingElections/Documents/Elections%20Division/Administration/Use%20of%20emergency_paper_ballots.pdf.

220 "Better Safe Than Sorry: How Election Officials Can Plan Ahead to Protect the Vote in the Face of a Cyberattack," Edgardo Cortés et al., Brennan Center for Justice, p. 3, https://www.brennancenter.org/sites/default/files/publications/08.15.18_Better_Safe_Than_Sorry.pdf.

221 "The 2014 EAC Election Administration and Voting Survey Comprehensive Report," U.S. Election Assistance Commission, https://www.eac.gov/assets/1/1/2014_EAC_EAVS_Comprehensive_Report_508_Compliant.pdf.

222 Emily Previti, "Voter Turnout in Pa. Primary up Slightly from Last Midterm," WHYY, May 17, 2018, https://whyy.org/articles/voter-turnout-in-pa-primary-up-slightly-from-last-midterm/.

223 "Better Safe Than Sorry: How Election Officials Can Plan Ahead to Protect the Vote in the Face of a Cyberattack," Edgardo Cortés et al., Brennan Center for Justice, p. 3, https://www.brennancenter.org/sites/default/files/publications/08.15.18_Better_Safe_Than_Sorry.pdf.

224 Oregon, for example, adopted remote accessible voting by mail that does not require Internet access to mark the ballot. Such a system could be used in a polling place in the event of machine failure. See "Voting Instructions for Voters with a Disability," State of Oregon, https://sos.oregon.gov/voting/Pages/instructions-disabilities.aspx.

225 "2018 Election Vulnerability: Voter Registration Systems," Nicholas Weaver, Lawfare blog, Feb. 23, 2018, https://www.lawfareblog.com/2018-election-vulnerability-voter-registration-systems.

226 "Better Safe Than Sorry: How Election Officials Can Plan Ahead to Protect the Vote in the Face of a Cyberattack," Edgardo Cortés et al., Brennan Center for Justice, p. 2, https://www.brennancenter.org/sites/default/files/publications/08.15.18_Better_Safe_Than_Sorry.pdf.

227 See generally "Election Security Advance Planning Checklist," Brennan Center for Justice, http://www.brennancenter.org/sites/default/files/publications/2018_08_13_ChecklistV4.pdf.

228 New Hampshire has a similar requirement. See, e.g., "New Hampshire Electronic Poll Books: Request for Information 2017–002," New Hampshire Secretary of State, p. 23, sos.nh.gov/WorkArea/DownloadAsset.aspx?id=8589969631 ("The electronic poll book shall have the ability to generate a paper voter checklist completely marked to reflect participation in the election up to the time of any system failure or malfunction.").

229 "The Election Administration and Voting Survey: 2016 Comprehensive Report," U.S. Election Assistance Commission, p. 28, https://www.eac.gov/assets/1/6/2016_EAVS_Comprehensive_Report.pdf.

The University of Pittsburgh is an affirmative action, equal opportunity institution. Published in cooperation with the Office of University Communications. 111627-0119

University of Pittsburgh

Institute for Cyber Law, Policy, and Security