University of Pittsburgh

THE BLUE RIBBON COMMISSION ON PENNSYLVANIA'S ELECTION SECURITY

STUDY AND RECOMMENDATIONS: IN BRIEF

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

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[1]

For the full report, visit: *www.cyber.pitt.edu/report*

1 Pennsylvania's election architecture 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	