Written Testimony Submitted to the State Government Committee
September 25, 2018

David Hickton and Paul McNulty
Co-Chairs, The Blue Ribbon Commission on Pennsylvania Election Security

Senator Folmer, Senator Williams, and members of the State Government Committee, we commend you for having this hearing and your attention to the critical issue of election security.

We write as the co-chairs of the independent, non-partisan Blue Ribbon Commission on Pennsylvania's Election Security to submit written testimony. Additional information about the Commission, its members, and its remit is appended. The Commission plans to release in early 2019 its final report assessing the cybersecurity of Pennsylvania's election architecture. We hope that it will provide useful information and recommendations to the General Assembly. In the meantime, we also include a set of the Commission's interim recommendations about voting systems.

Today, we write with four main points:

(1) The majority of Pennsylvania's voting systems must be urgently replaced.
(2) The General Assembly should assist counties in funding these replacements.
(3) The General Assembly should amend the election code to provide for statistically sound risk-limiting audits.
(4) The General Assembly should continue proper oversight of the security of Pennsylvania's election architecture.

1. Pennsylvania Counties Must Replace Vulnerable Voting Machines

The bulk of Pennsylvania's voting machines are vulnerable to hacking and manipulation, and this has long been demonstrated by computer scientists.[1] While there is not evidence to support

[1] *See, e.g.*, National Academies of Sciences, Engineering, and Medicine. 2018, *Securing the Vote: Protecting American Democracy*, Washington, DC: The National Academies Press, https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy; US Senate Select Intelligence Committee, *Russian Targeting of Election Infrastructure During the 2016 Election, Summary of Draft SSCI Recommendations*, March 20, 2018, https://www.burr.senate.gov/imo/media/doc/One-Pager%20Recs%20FINAL%20VERSION%203-20.pdf; Brennan Center for Justice, *Voting Machines at Risk – An Update*, March 8, 2018, https://www.brennancenter.org/analysis/americas-voting-machines-risk-an-update#_ednref8;

the conclusion that 2016 election results were compromised, the risk remains and it is imperative that steps be taken to eliminate this vulnerability.

Pennsylvania is one of the states most vulnerable to both election manipulation and election-day disruptions because most of its counties rely on insecure electronic voting machines that are susceptible to manipulation and offer no paper record—and therefore no way of verifying the tabulation of votes where the veracity of election results is questioned. Nor can these machines support meaningful recounts.

Computer scientists and cybersecurity experts, as well as most election administration officials, agree that the most insecure voting machines are "DRE's without VVPAT" (Direct Recording Electronic systems *without* a Voter-Verifiable Paper Audit Trail) machines. There is a remarkable consensus of experts around the insecurity of these machines.[2] Unfortunately, however, 83 percent of Commonwealth voters use these particularly vulnerable computerized voting systems.[3]

Exacerbating the security vulnerabilities of DRE machines without voter-verifiable paper audit trails is the inability to conduct a meaningful post-election audit of the results. In other words, if the records are corrupted (intentionally by malicious attack or from benign malfunction), there is no way to know. The US Department of Homeland Security Secretary Kirstjen Nielsen testified

---

Wofford, Ben. "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.*, election integrity expert letter to Congress, 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," signed by over 100 cybersecurity and voting experts. *See also*, National Academies of Sciences, Engineering, and Medicine. 2018. *Securing the Vote: Protecting American Democracy*. Washington, DC: The National Academies Press. https://doi.org10.17226/25120; Testimony of Dr. 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, Computer and Information Science, University of Pennsylvania, Before the US 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 F. Hao and P.Y.A. Ryan (eds.), *Real-World Electronic Voting: Design, Analysis, and Deployment*, CRC Press, December 2016.

[3] Verified Voting: https://www.verifiedvoting.org/verifier/.

before the US Senate Select Intelligence Committee that the inability to audit election results in states such as Pennsylvania poses a threat to national security.[4]

Without a method to conduct meaningful audits of election results,[5] an attack would not have to change the outcome of the vote to impact the public's faith in the reported outcome of the vote. If a county cannot credibly prove that the outcome of its vote is accurate, the assertion of a successful hack could have the potential to be just as damaging as the reality of a successful hack. Election officials would lack the means to demonstrate to the public that the vote was not compromised.

As Rice University computer scientist and election security expert Dan Wallach suggested in Congressional testimony:

> 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.[6]

Here in Pennsylvania, the Advisory Committee on Voting Technology to the Joint State Government Commission found that, "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

---

[4] Volz, Dustin 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." Sec'y Kirstjen M. Nielsen, Remarks to the National Election Security Summit, September 10, 2018, https://www.dhs.gov/news/2018/09/10/secretary-kirstjen-m-nielsen-remarks-national-election-security-summit (emphasis added).

[5] 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 is correct. However, these actions will not uncover errors or interference in the tabulation software and the inability to detect those errors could impact the outcome of the election contest.

[6] Testimony of Dr. 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 & 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.

that facilitates post-election audits and recounts, is the best means of maintaining voter confidence."[7]

Best practice for electronic voting systems is now widely considered paper ballots either filled out by the voter or marked using a ballot-marking device and then tabulated by optical scanners.[8] Optical scan systems provide us the assurance of auditability, and, if necessary, a recount.[9]

Pennsylvania therefore took a significant step forward in improving its election security when Acting Secretary of State Robert Torres directed on April 12, 2018, that all Pennsylvania counties have "voter-verifiable paper record voting systems selected no later than December 31,

---

[7] "Voting Technology in Pennsylvania" Report of the Advisory Committee on Voting Technology, December 2017, at 66, available here: http://jsg.legis.state.pa.us/publications.cfm?JSPU_PUBLN_ID=463.

[8] *See*, *e.g.,* National Academies of Sciences, Engineering, and Medicine. 2018, *Securing the Vote: Protecting American Democracy*, Recommendation 4.11, Washington, DC: The National Academies Press, 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, Computer and Information Science, University of Pennsylvania, Before the US 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 Dr. 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 Dr. 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 & 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.

[9] 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.,* National Academies of Sciences, Engineering, and Medicine, 2018, *Securing the Vote: Protecting American Democracy*, Recommendation 5.5, Washington, DC: The National Academies Press, 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."). We do not recommend systems with bar codes or QR codes as these are not human readable.

2019, and preferably in place by the November 2019 general election."[10] Per an earlier directive, any elections systems purchased February 9, 2018 onward must include a paper audit capacity.[11]

2. The General Assembly should assist counties in funding these replacements.

The cost of procuring new voting machine systems is not trivial. In April, the Wolf Administration estimated that outright purchasing of new voting machines to replace paperless DREs could cost between $95 - $153 million statewide.[12] The County Commissioner's Association estimates the cost at $125 million.[13] This is a cost of $9.76 per Pennsylvania citizen.

The cost of doing nothing, however, is potentially far higher. Faith in our election results, once lost, will be difficult to regain.

The new funding the US Congress approved in March 2018 included $13.5 million for Pennsylvania.[14] The Commonwealth's required matching funds bring this to $14.2 million, all of which the Commonwealth is providing to counties for the purchase of new voting systems. While we hope (and strongly urge) that additional federal funding will be forthcoming, this is not something that the State or its counties should rely on. Without assistance from the General Assembly, counties will be bearing the cost of replacing voting systems.

When we consider the cost of replacing existing systems, it is important to note that most of the electronic voting systems in use in Pennsylvania are nearing or have passed the end of their usable lives. In other words, counties would need to replace these systems within the next few years regardless of the administration's directive.

We therefore respectfully urge the General Assembly to consider substantial cost-sharing with the counties. This could include exploring the possibility of bonds as a financing mode for the purchase of new voting equipment.

---

[10] Department of State. (2018, April 12). *Department of State Tells Counties to Have New Voting Systems in Place by End of 2019* [Press release]. Retrieved from http://www.media.pa.gov/Pages/State-Details.aspx?newsid=276.

[11] Department of State. (2018, February 9). *Wolf Administration Directs that New Voting Systems in the Commonwealth Provide Paper Record* [Press release]. Retrieved from http://www.media.pa.gov/Pages/State-Details.aspx?newsid=261.

[12] PennLive.com, "Q&A: What Will Have to be Done to Upgrade PA's Voting Systems?." *Pennlive*, April 13, 2018. Accessed at: http://www.pennlive.com/news/2018/04/qa_what_will_have_to_be_done_t.html.

[13] County Commissioners Association of Pennsylvania. (2018, April 13). *Counties React to DOS Voting Equipment Directive* [Press release]. Retrieved from 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.

[14] Brennan Center for Justice. (2018, March 22). *Proposed Election Infrastructure Spending*. Accessed at https://www.brennancenter.org/analysis/proposed-election-infrastructure-spending.

Election reforms that address the way in which Pennsylvania conducts elections could also help identify inefficiencies in election budgets. The Advisory Committee on Voting Technology to the Joint State Government Commission provides recommendations,[15] as does the County Commissioners Association of Pennsylvania.

We note that this should not be considered a one-time cost for replacement. A 10-15 year cycle of replacement of voting systems will likely be the new normal. The General Assembly and the Governor's office should therefore work together to create a new permanent election security fund, which accrues money annually and can be used as needed, whether for equipment, trainings, security assessments, or otherwise.

3. **The General Assembly should amend the election code to provide for statistically sound risk-limiting audits.**

It is not enough to protect against compromised voting machines. All machines can suffer from exploitable vulnerabilities. Therefore, election security experts recommend implementing risk-limiting audits to determine whether reports from voting machines and tabulation systems included any errors. Election security experts nearly universally agree that paper ballots via optical scan systems paired with risk-limiting audits are the gold standard in election security.[16]

These risk-limiting audits, in which officials check a random sample of paper ballots against digital tallies to ensure the results were tabulated correctly, allow officials to detect software

---

[15] "Voting Technology in Pennsylvania" Report of the Advisory Committee on Voting Technology, December 2017. Accessed at http://jsg.legis.state.pa.us/publications.cfm?JSPU_PUBLN_ID=463.

[16] *See, e.g.*, National Academies of Sciences, Engineering, and Medicine, 2018, *Securing the Vote: Protecting American Democracy*, Recommendations 4.11-13, 5.5-10, Washington, DC: The National Academies Press, https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy; Testimony of Dr. 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, Computer and Information Science, University of Pennsylvania, Before the US 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 Dr. 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 & 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; Brennan Center for Justice, Common Cause, National Election Defense Coalition, VerifiedVoting, *Securing the Nation's Voting Machines*, May 31, 2018, https://www.brennancenter.org/publication/securing-nations-voting-machines.

failures and attacks, including those that might have been initiated within the supply chain.[17] The 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.

Pennsylvania law currently requires a recount of a random sample of the lesser of 2 percent of votes cast in a county, or 2,000 ballots.[18] Given that most Pennsylvania counties currently use DRE voting systems without voter-verifiable paper audit trails, performing this kind of audit is impossible. No true audit can be made as this audits only the machines' ability to add, not its ability to correctly interpret and preserve voter's intent. A recount of a paperless voting machine cannot catch corrupted records, whether corrupted by malicious intent or benign error.

Put simply, because there are no actual individually-marked ballots to audit, election officials cannot meet the election code's requirement of a recount with paperless DRE machines.

Instead of a fixed-percentage audit, in combination with moving to paper-record voting systems, Pennsylvania should institute risk-limiting audits for every election. As University of Pennsylvania computer scientist Matt Blaze describes it, "[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."[19]

Risk-limiting audits are designed to provide strong evidence that tabulation errors have not altered the outcomes in particular contests. The risk limit 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. A risk-limiting audit continues until strong evidence exists that the tabulation outcome is correct – or, if necessary, a full hand count is conducted to determine the correct outcome. Unlike fixed-percentage audits, risk-limiting audits generally require hand counts of fewer ballots for contests with large margins than contests with small margins.[20] Thus,

---

[17] Lindeman, Mark and Philip B. Stark. A Gentle Introduction to Risk Limiting Audits. (2012, March 26). *IEEE Security and Privacy, Special Issue on Electronic Voting*. Accessed at https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf; Christopher Deluzio, *A Smart and Effective Way to Safeguard Elections*, July 25, 2018, https://www.brennancenter.org/publication/securing-nations-voting-machines (discussing risk-limiting audits).

[18] Pa. Cons. Stat. Tit. 25 Sec. 3031.17.

[19] Testimony of Matthew Blaze, Associate Professor, Computer and Information Science, University of Pennsylvania, Before the US 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.

[20] Lindeman, Mark and Philip B. Stark. A Gentle Introduction to Risk Limiting Audits. (2012, March 26). *IEEE Security and Privacy, Special Issue on Electronic Voting*. Accessed at https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf; Christopher Deluzio, *A Smart and Effective Way to Safeguard Elections*, July 25, 2018,

risk-limiting audits are considered more efficient than traditional post-election audits, which tend to require that a set number of ballots be audited regardless of the margin of victory in a given race.

Risk-limiting audits detect mistakes in election outcomes more consistently than traditional audits. Risk-limiting audits also can be less expensive because they often need to sample fewer ballots.

Colorado recently instituted the requirement that all elections be subject to a risk-limiting audit,[21] becoming the first state to carry out mandatory post-election audits in 2017.[22] The open-source audit software used in Colorado is available for free and can be customized for other states.[23] Rhode Island also passed a bill requiring risk-limiting post-election audits for future elections.[24] Both states provide good examples that could be used, with some adaptations, for Pennsylvania's particular election requirements.

Risk-limiting audits, if implemented transparently and conducted for every election, would be a critical part of building confidence in Pennsylvania's elections, even in the face of threats of attacks or disinformation campaigns.

We therefore urge the Department of State to pilot risk-limiting audits in partnership with those counties that already use optical scan voting systems. Following pilots, we recommend that the General Assembly mandate risk-limiting audits for every election in Pennsylvania.

4. **The General Assembly should continue proper oversight of the security of Pennsylvania's election architecture.**

---

https://www.brennancenter.org/publication/securing-nations-voting-machines ("Because risk-limiting audits take into account both the margin of victory and the total number of votes cast and use principles of statistics, these 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.").

[21] Election Rules, 8 CCR 1505-1, Rule 25, Post-Election Audit, accessed at http://www.sos.state.co.us/pubs/rule_making/CurrentRules/8CCR1505-1/Rule25.pdf.

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

[23] The Colorado Risk-Limiting Audit Project (CORLA). Retrieved from http://bcn.boulder.co.us/~neal/elections/corla/.

[24] RI Gen L Sec. 17-19-37.4 (2017). Virginia also has a statutory requirement for risk-limiting audits. *See* http://lis.virginia.gov/cgi-bin/legp604.exe?171+ful+CHAP0367+pdf; New Mexico also carries out some risk-limiting audits.

We were pleased to see the introduction of Senate Bill 1249, which provides for a Pennsylvania Election Law Advisory Board. We hope that this will provide an opportunity to study updating the Election Code for improving election administration, including cost savings measures, as well as for introducing risk-limiting audits.

We appreciate the thoughtful representation on the board and would also encourage the inclusion of cybersecurity experts in the members representing each congressional district to be appointed by the Governor.

While we would urge the appointment of this Committee, its existence and work should not offer an opportunity for delay in replacing insecure and outdated voting systems here in Pennsylvania.

In conclusion, we commend you for holding this hearing and for bringing attention to the critical issue of Pennsylvania's election security. We hope that The Blue Ribbon Commission on Pennsylvania's Election Security can be of assistance to the General Assembly on these issues.

The Blue Ribbon Commission on Pennsylvania's Election Security

– Interim Recommendations on Voting Systems –

There is *no* publicly available evidence of successful hacking of the 2016 US elections, in Pennsylvania or elsewhere. However, there is also no question that Pennsylvania's elections, like other states, are under threat.

This is not a partisan issue. All Pennsylvanians should be concerned about the current status quo with respect to the cybersecurity of our elections. By multiple assessments, Pennsylvania is one of the states most vulnerable to election manipulation or election-day technical problems, in large part because of its reliance on older electronic voting systems. An estimated 83 percent of Pennsylvanians vote on machines that offer no auditable paper record. The lack of an auditable record could prevent Pennsylvania's counties from detecting a successful hacking or even benign error, and prevents counties from recovering in such an event. As the US Secretary of the Department of Homeland Security Kierstjen Nielsen has testified, not having a verifiable way to audit election results is a "national security concern."

Manipulating voting machines is one feasible method of an attack on our elections—and one that should be guarded against. Pennsylvania therefore took a significant step forward in improving its election security when Acting Secretary of State Robert Torres 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." Per an earlier directive, any elections systems purchased February 9, 2018 onward must include a paper audit capacity.

These actions and others by Governor Wolf's Administration bode well for the future of Pennsylvania's election security. It deserves credit for thoughtful and thorough ongoing attention to the issue.

Local election officials also deserve thanks from all of us living in the Commonwealth for their commitment to the extraordinary effort that is administering our elections—and now the tremendous responsibility of securing them from nation-state adversaries.

However, additional actions from the Governor and Secretary of State, the General Assembly, and counties will be needed to ensure the security of Pennsylvania's vote—and citizens' faith therein.

With this in mind, the Blue Ribbon Commission on Pennsylvania's Election Security has undertaken a study of Pennsylvania's preparedness. Our full report and recommendations will be issued in early 2019. However, given the urgency of the threat and that many counties are appropriately undertaking decisions with respect to replacing outdated voting systems, the Commission has decided to issue interim recommendations with respect to new voting systems.

We note with caution that while voting systems often receive the most attention from media reports, efforts are also needed to secure Pennsylvania's election security throughout the broader election architecture. This includes the security of election management systems; the voter registration system; and response and recovery in the event of a cyber incident, including disinformation campaigns. Our 2019 report will include full attention to these issues, in addition to a more fulsome discussion of voting systems and improving Pennsylvania's election audits.

Recommendations:

(1) Counties Should Replace Vulnerable Voting Machines.

- Those counties using DREs without voter-verifiable paper audit trails 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.

(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 Pennsylvanian's faith in them—are not free.

- The General Assembly should appropriate funding to help cover the cost of counties' purchasing voting systems with voter-marked paper ballots (either by hand or by machine) and other needed improvements to Pennsylvania's election security. It should also consider creating a fund for regular future appropriations as upgrades in security and accessibility technologies merit.

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

(3) Follow Vendor Selection and Management Best Practices To Minimize Supply Chain Vulnerabilities.

- As election officials work with vendors on a range of items affecting the election architecture, including ballot preparation, logic and accuracy testing, and equipment procurement, it is imperative to safeguard against supply chain vulnerabilities and to assess vendors for potential security risks. This includes using a vendor's cybersecurity readiness as a primary metric in procurement decision-making and conducting ongoing cybersecurity monitoring throughout the life cycle of the vendor relationship.

Pennsylvania's elections are at risk. And one of the biggest risks is one that we can control—properly funding our election security, including by procuring voting machines that use voter-marked paper ballots.

We recognize that the General Assembly and counties have many funding priorities. The County Commission Association of Pennsylvania estimates the cost for replacing voting machines to be $125 million statewide. The majority of Pennsylvania's current voting machines leave the integrity of our Commonwealth's vote at risk. This is unacceptable. Compared to the magnitude of this risk, $125 million is a relative bargain.

Pennsylvania, like any other state, cannot entirely eliminate the risk of cyberattack or other errors on its computerized voting systems. However, it can work to both reduce the potential for attack and mitigate its impact in the instance of an attack. The faith in the integrity of our elections is at stake. Once shaken, it will be difficult to restore.

The Blue Ribbon Commission on Pennsylvania's Election Security

David Hickton – Founding Director, Pitt Cyber; former US Attorney for the Western District of Pennsylvania (co-chair)

Paul McNulty – President, Grove City College; former Deputy Attorney General of the United States; former US Attorney for the Eastern District of Virginia (co-chair)

Jim Brown – Former Chief of Staff to US 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, US 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 State 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

Peri Jude Radecic – CEO, Disability Rights Pennsylvania

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 Secretary 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 US 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

Senior Advisors

Charlie Dent – Former US Congressman, 15th District of Pennsylvania

Paul H. O'Neill – 72nd Secretary of the US Treasury

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

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

About the Commission: The Blue Ribbon Commission on Pennsylvania's Election Security is an independent, non-partisan commission studying Pennsylvania's election cybersecurity, hosted by the University of Pittsburgh Institute for Cyber Law, Policy, and Security (Pitt Cyber). We are grateful for the generous support of The Heinz Endowments and the Charles H. Spang Fund of The Pittsburgh Foundation and for collaboration between Pitt Cyber, Carnegie Mellon's Software Engineering Institute CERT Division, and Verified Voting.