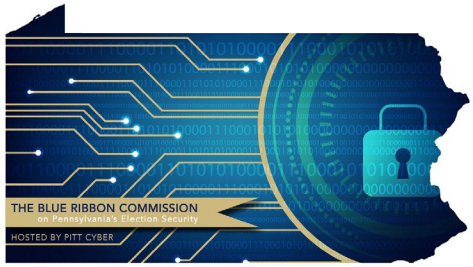

Written Testimony Submitted to the House State Government Committee
October 15, 2018

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

Representative Metcalfe, Representative Bradford, and members of the House State Government Committee, we commend you for bringing attention to the critical issue of the security of Pennsylvania's voter rolls.

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.

The Pennsylvania Department of State deserves credit for steps taken in improving the cybersecurity of the voter registration system since 2016, as well as for its partnership with the Auditor General going forward in ensuring cybersecurity best practices with respect to the replacement system.

Today, we write with four main points:

(1) State voter registration databases are targets for cyberattack.
(2) Pennsylvania's voter registration system has cyber-related vulnerabilities.
(3) The General Assembly should support improvements to and the forthcoming replacement of Pennsylvania's voter registration system.
(4) The General Assembly should support counties' urgent replacement of the majority of Pennsylvania's voting systems and institute risk-limiting audits after each election.

1. State voter registration databases are targets for cyberattack.

Although voting machines—and the significant threats posed to the security of machines—have recently garnered significant media attention (and perhaps pose the gravest short-term risk to the security of Pennsylvania's elections), voter registration systems were specifically targeted for cyberattack in the lead-up to the 2016 presidential election. 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.[1] At least 18 states—and perhaps as many as 21—"had election systems targeted by Russian-affiliated cyber actors."[2] That targeting included "vulnerability scanning directed at…Secretary of State websites or voter registration infrastructure."[3]

According to the Department of Homeland Security, Pennsylvania was one of the states whose voter registration system was targeted by the Russians.[4] However, per the Wolf Administration, "neither it nor the U.S. Department of Homeland Security has any evidence of a breach."[5] The system—known as the Statewide Uniform Registry of Electors (SURE)—was probed, but the publicly available evidence suggests SURE was not penetrated.

Malicious access attempts were *detected* 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."[6] There of course may have been other attempts (including in Pennsylvania perhaps) that remain undetected. Moreover, the Justice Department's recent indictment of Russian hackers alleged that the Russians successfully hacked a state election website and stole sensitive information for half a million voters.[7] 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."[8]

Notwithstanding the gravity of these threats, the risk of alteration of voter registration records in SURE is low because voters would presumably learn of changes to records at the latest when they show up to vote. Moreover, if Pennsylvania counties that do not use paper ballots transition to voting machines that use a paper ballot marked by the voter (either manually or with a ballot marking device) and post-election risk-limiting audits are adopted, these measures will substantially increase the likelihood of not only detecting an attack of SURE but also correcting any altered outcomes by recounting voter-verified paper ballots.

---

[1] Report of U.S. Senate Intelligence Committee, *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations*, May 8, 2018, https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf.

[2] *Id.*

[3] *Id.*

[4] Nat'l Ass'n of Secs. of State, *DHS State Notification and State Public Statements*, Sept. 29, 2017, https://www.nass.org/sites/default/files/chart-dhs-state-notifications-public-statements092917.pdf.

[5] Associated Press, Russians Targeted Pennsylvania Election System, State Told, Sept. 22, 2017, https://www.pennlive.com/politics/index.ssf/2017/09/russians_targeted_pennsylvania.html.

[6] Report of U.S. Senate Intelligence Committee, *Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations*, May 8, 2018, https://www.burr.senate.gov/imo/media/doc/RussRptInstlmt1-%20ElecSec%20Findings,Recs2.pdf.

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

[8] *Id*. ¶ 73.

However, even attacks that fail to alter the ultimate results of an election could nonetheless succeed in damaging public trust in the outcome or disrupting administration of the election without necessarily altering the ultimate outcome of the vote. Either could undermine faith in democracy in Pennsylvania.

2. Pennsylvania's voter registration system has cyber-related vulnerabilities.

As of June 2017, 41 states (including Pennsylvania) were still using voter registration databases that were initially created a decade ago or longer.[9] As the Brennan Center has observed, "[t]hese outdated systems were not designed to withstand current cybersecurity threats."[10] 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, and Pennsylvania is poised to update and replace the system in the next three or so years (and, as discussed below, has already kicked off the preliminary procurement process). In the meantime, however, there are current threats to and vulnerabilities of SURE that must be addressed.

Although this testimony does not purport to address all such issues, there are two in particular that merit discussion: (1) alterations, deletions, or creations of registrations and (2) DDoS attacks.

In a recent paper, researchers from Carnegie Mellon University analyzed potential vulnerabilities in Pennsylvania's entire election ecosystem—with a particular focus on Allegheny County.[11] The researchers identified specific attack scenarios targeting Pennsylvania's voter registration system with potential statewide ramifications.

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 of their Social Security number—the report identified a "major vulnerability."[12] That vulnerability stems from the availability of driver's license and Social Security numbers "on sites like Pastebin or for purchase on the dark web."[13] The easily obtainable state voter file (which can be purchased for $20[14]) and SURE's polling place location tool (accessible via the Internet[15]) could further aid

---

[9] Wendy Weiser & Max Feldman, Brennan Ctr. for Justice, *The State of Voting 2018*, https://www.brennancenter.org/sites/default/files/publications/2018_06_StateOfVoting_v5%20%281%29.pdf.

[10] *Id.*

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

[12] *Id.* at 5.

[13] *Id.* at 6.

[14] Pa. Dep't of State, PA Full Voter Export, https://www.pavoterservices.pa.gov/pages/purchasepafullvoterexport.aspx.

[15] Pa. Dep't of State, Find Your Polling Place, https://www.pavoterservices.pa.gov/pages/pollingplaceinfo.aspx.

would-be attackers looking to target SURE.[16] Armed with voters' personal information, nefarious actors could create fake registrants or modify existing records by changing a name, address, or party affiliation. 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 attack scale.

Similarly, a 2017 paper by Harvard researchers argued that hackers could mount a coordinated campaign of voter identity theft using targeted states to submit false changes to actual voter records, albeit through a laborious process of changing individuals' information one-by one.[17] 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.[18] Election officials strongly disputed some of the paper's findings, stressing that safeguards—like automated security features of registration websites, mailing written confirmations to those whose registrations were changed online, and other measures to detect and prevent bulk changes to voters' registration records—were already broadly in place across the country.[19]

Most experts agree that nefarious registration record changes 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.

Another key threat is a Distributed Denial of Service (DDoS) attack on public-facing voter registration 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."[20] Such an attack could prevent

---

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

[17] Latanya Sweeney et al, *Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections*, Sept. 6, 2017, https://techscience.org/a/2017090601/.

[18] *Id.* at 95.

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

[20] U.S. Dep't of Homeland Sec., Security Tip (ST04-015), Understanding Denial-of-Service Attacks, Nov. 4, 2009, https://www.us-cert.gov/ncas/tips/ST04-015.

"voters from registering and potentially discourage[e] them from participation."[21] 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 guarded against.

3. The General Assembly should support improvements to and eventual replacement of Pennsylvania's voter registration system.

The Commonwealth is poised to embark upon the process to replace the existing voter registration system (SURE).[22] This procurement process will give Pennsylvania an excellent opportunity to deploy best practices in selecting, developing, and implementing a registration system designed to guard against a range of cybersecurity threats. In another positive development, Pennsylvania Auditor General Eugene DePasquale recently announced that his office would conduct an audit of Pennsylvania's voter registration and voting systems.[23] This audit will be part of an interagency agreement with the Department of State, with recommendations planned to be issued in time to be implemented prior to the 2020 election.[24] Ideally, the audit's findings ought to be leveraged to inform the procurement process to replace SURE.

In connection with the replacement of SURE, we urge the General Assembly first and foremost to support the Department of State's forthcoming procurement process with needed appropriations.

In fulfilling its oversight role, we also recommend that the General Assembly ensure that the Department of State heeds cybersecurity best practices in its dealings with vendors, such as those

---

[21] Harvard Kennedy School, Belfer Ctr. for Sci. and Int'l Affairs, The State and Local Election Cybersecurity Playbook at 28, https://www.belfercenter.org/sites/default/files/files/publication/StateLocalPlaybook%201.1.pdf.

[22] Pa. Bureau of Procurement, Supplier Service Center, PA e-Marketplace, http://www.emarketplace.state.pa.us/Solicitations.aspx?SID=6100044816-SF (Statewide Uniform Registry of Electors System procurement solicitation).

[23] Press Release, Pa. Dep't of the Auditor Gen., *Auditor General DePasquale Expands Scope of Voting Security Audit Outreach in Wake of Latest Indictments of Russian Hackers*, July 17, 2018, https://www.paauditor.gov/press-releases/auditor-general-depasquale-expands-scope-of-voting-security-audit-outreach-in-wake-of-latest-indictments-of-russian-hackers.

[24] Press Release, Pa. Dep't of the Auditor Gen., *Auditor General DePasquale Launches Audit to Safeguard Voting Security*, June 11, 2018, http://www.paauditor.gov/press-releases/auditor-general-depasquale-launches-audit-to-safeguard-voting-security.

suggested by the U.S Department of Homeland Security[25] and the Center for Internet Security.[26] Vendor cybersecurity practices and consideration of supply-chain vulnerabilities should be key factors weighed by the Department of State in selecting vendors. We also urge the General Assembly to encourage that the Department of State work closely with the Auditor General's office in connection with their audit of Pennsylvania's election systems. Close collaboration and cooperation could arm Department of State personnel with detailed knowledge about any audit findings that ought to be considered in and used to inform the SURE procurement process, specifically. Moreover, we would urge close consultation with the newly-formed Inter-Agency Election Preparedness and Security Workgroup, which is led by co-chairs Robert Torres (Acting Secretary of State) and John MacMillan (Deputy Secretary for Information Technology and Chief Information Officer), and the county/Commonwealth election security workgroup. In addition, should Senate Bill 1249—which provides for a Pennsylvania Election Law Advisory Board and an opportunity to study updating the Election Code for improving election administration, including cost savings measures and introducing risk-limiting audits—become law, we would similarly urge close collaboration with the Board.[27]

In the meantime, there are several enhancements to the SURE system that could bolster its cybersecurity. Implementation of multi-factor authentication could mitigate a vulnerability in SURE whereby nefarious actors with access to personal identifying information could erroneously change voter registration record. The Department of State should consider such an authentication method—presumably by verifying a piece of information that was provided upon application for registration. It would be 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. In addition, the Department of State should consider adding a second layer of encryption to data in the SURE system. At present, data is already 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 itself within the encrypted hardware.[28] Lastly, we recommend requiring that a paper notification letter be mailed to registrants on Pennsylvania's online voter registration application who are changing their address. For registrants changing their address, a letter should be sent to both the old and the new address.

---

[25] U.S. Dep't of Homeland Sec., *DHS Election Infrastructure Security Funding Consideration*, June 13, 2018, https://www.dhs.gov/sites/default/files/publications/Election%20Infrastructure%20Security%20Funding%20Considerations%20Final.pdf.

[26] Ctr. for Internet Sec., *A Handbook for Elections Infrastructure Security*, Feb. 2018, https://www.cisecurity.org/wp-content/uploads/2018/03/CIS-Elections-Handbook-19-March-Single-Pgs.pdf.

[27] With respect to the composition of the Pennsylvania Election Law Advisory Board, we encourage the inclusion of cybersecurity experts in the members representing each congressional district to be appointed by the Governor.

[28] The Department of State is already considering implementation of this added level of encryption.

4. **The General Assembly should support counties' urgent replacement of the majority of Pennsylvania's voting systems and should institute risk-limiting audits after each election.**

Although the vulnerabilities in the voter registration system are serious, the risk associated with Pennsylvania's DRE machines presents a more clear and present danger to the integrity of the vote.

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.[29] Unfortunately, however, 83 percent of Commonwealth voters use these particularly vulnerable computerized voting systems.[30]

These paperless machines leave officials without a method to conduct meaningful audits of election results.[31] Consequently, 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.

---

[29] *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.

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

[31] 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.

It is imperative that election officials have the ability to demonstrate to the public that electoral outcomes are correct—something that paper ballots coupled with mandatory post-election audits can provide. Not only would this improve election security, it would also lessen the risk of erosion of public trust in elections flowing from a registration-related cyber incident or technological error. So too would paper ballots and post-election audits increase the likelihood of detecting a registration-based attack on the vote.

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."[32] Per an earlier directive, any elections systems purchased February 9, 2018 onward must include a paper audit capacity.[33]

Yet 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.[34] The County Commissioner's Association estimates the cost at $125 million.[35] 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. 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.

It is not enough to replace vulnerable voting machines—Pennsylvania should also institute mandatory risk-limiting audits after every election.

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

---

[32] 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.

[33] 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.

[34] 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.

[35] 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.

universally agree that paper ballots via optical scan systems paired with risk-limiting audits are the gold standard in election security.[36]
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 failures and attacks, including those that might have been initiated within the supply chain.[37] 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.

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.

---

[36] *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, Verified Voting, *Securing the Nation's Voting Machines*, May 31, 2018, https://www.brennancenter.org/publication/securing-nations-voting-machines.

[37] 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).

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.