COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF STATE

Testimony of Kathy Boockvar
Acting Secretary of the Commonwealth
Commonwealth of Pennsylvania
Hearing on *Securing America's Elections*
U.S. House of Representatives, Committee on the Judiciary
September 27, 2019

Chairman Nadler, Ranking Member Collins, and distinguished members of the House Judiciary Committee, my name is Kathy Boockvar, and I am the acting Secretary of State (or Secretary of the Commonwealth) of Pennsylvania. As Secretary, I lead the Pennsylvania Department of State (DOS) to promote the integrity and security of the electoral process, protect public health and safety by licensing professionals, support economic and nonprofit development through corporate and charitable registrations, and sanction professional boxing, kick-boxing, wrestling and mixed martial arts. Prior to being appointed as Secretary, I served as Senior Advisor to Governor Wolf on Election Modernization, leading and managing initiatives to improve security and technology in Pennsylvania's elections, in collaboration with federal, state, and county officials.

Thank you for inviting me to testify at your *Securing America's Elections* hearing. As the Chief Election Official of Pennsylvania I have the immense privilege of working with extraordinarily dedicated election directors and personnel in all 67 counties across the Commonwealth, as well as committed Secretaries of State across our great nation, to ensure that our elections - elections that allow candidates running for every local, state, and federal office to serve – are free, fair, secure, and accessible to all eligible voters. In August 2019, I was also honored to be asked to serve as the Elections Committee Co-Chair for the National Association of Secretaries of State (NASS).

The issues surrounding security have made election administration more challenging and complex than ever. As we have learned over the last several years, foreign adversaries and other cyber actors have attempted and continue to attempt to influence elections in the United States. The key to thwarting this effort is that we must continue to build and strengthen our walls faster than those that are trying to tear them down. Election security is a race without a finish line, and our adversaries are continuously advancing their technologies. We must do the same and more; our success is dependent on substantial and sustained dedication of resources.

Alongside the great majority of states across the nation, we urge the federal government to provide additional election security funding and support to counties and states and reinforce our collective infrastructure. All of us at the federal, state, and local levels benefit from the security of our elections, so funding these critical operations must be a cost-share by the federal, state, and local levels. Because the technologies and attempted attacks are becoming more

sophisticated all the time, we need to plan for and invest in election security like we invest in other ongoing initiatives and challenges. Like other types of security, like STEM fields, like education of our children – investment cannot be once and done, and it should never be dependent on political winds. There is nothing partisan about ensuring that our elections are secure and accessible to all eligible voters. We must have a continuous investment in election security at all levels, both in funding and in strengthening our infrastructure, communications, and responsiveness, so that we may advance and adapt to change as new information is gained and new technologies advanced.

NATIONAL LANDSCAPE

There have been some great advances in election security over the last several years at all levels, while challenges continue to emerge as well. All these – continuing to strengthen advances and pursuing additional goals forward - require significant funding, proactive bi-partisan leadership, quick response time, multi-agency collaboration, and other support.

The National Association of Secretaries of State (NASS), National Association of State Election Directors (NASED) and Secretaries and election officials across the country have been resolute in our commitment to bolstering security in elections, and collaboration at all levels. As NASS Elections Committee Co-Chair, I look forward to working with my fellow Co-Chair Secretary Mac Warner (W.Va.) and with colleagues across the country, to share best practices and provide the most secure and accessible elections to eligible voters in Pennsylvania and nationwide. One of my responsibilities as Co-Chair is to serve as a NASS representative on the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC).

In January 2017, when the federal government designated election infrastructure as part of the nation's critical infrastructure, the EIS-GCC was one of the first developments of that designation. The EIS-GCC is a first of its kind collaboration among federal, state, and local officials to secure elections, working to formalize and improve information-sharing and communication protocols to ensure that timely threat information, support, and resources reach all election officials so they can respond to threats as they emerge. The EIS-GCC has 29 members, of which 24 are state and local election officials. It also includes members from the U.S. Department of Homeland Security (DHS), the U.S. Election Assistance Commission, the National Association of State Election Directors (NASED), the Election Center, and the International Association of Government Officials. The members of the EIS-GCC are working to update an elections-sector specific plan, improve communications protocols and portals, and secure increased resources for state and local election officials. In addition to the GCC, a Sector Coordinating Council (SCC) was also established for non-government, private sector entities to better communicate with election officials and the federal government.

Beyond the EIS-GCC, DHS and the Center for Internet Security (CIS) have been particularly strong partners. Pennsylvania and other states regularly collaborate with DHS on independent risk and vulnerability assessments, intelligence, training, tabletop exercises, communications,

and more. We also work with CIS's Multi-State Information Sharing and Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing and Analysis Center, (EI-ISAC) to gather and share intelligence about cyber threats that target government or government-affiliated systems, and gain support and resources including forensic analyses and emergency response assistance. Additionally, the cyber defense team of the Pennsylvania National Guard has been an exceptionally strong partner. Within the last year they were the first National Guard team selected to participate in a new DHS program, to be trained to conduct Risk and Vulnerability Assessments to DHS standards.

For all these strong collaborative partnerships to be most effective, and for additional goals to be advanced, more resources are needed. Some top priorities would include the federal government playing a greater role with vendor oversight, including tracking vendor foreign ownership, data hosting, manufacturing and employee background checks, and chain of custody for all voting and election system components; and reinforcing Continuity of Operations Plans (COOP) across levels and sectors, to provide more clarity on primary points of contact in the federal government for incidents and concerns. It would also be beneficial to have broader communications between our federal election security partners and our state legislatures and counties, so that counties and legislators could hear directly about federal election security priorities and concerns. We also need to strengthen lines of communication from the federal government to the state chief election officials, for example to ensure that federal entities notify the state when local incidents are reported, so that we may immediately act when necessary. Additionally, federal funding and support are needed to ensure that all counties have state-of-the-art intrusion detection systems, comprehensive phishing, cyber hygiene, and security awareness training, vulnerability assessments, and more.

PENNSYLVANIA LANDSCAPE

Most people have an understanding that the word "cyber" relates to the study of systems and the intersections and communications between people and machines. But the word "cyber" actually has ancient Greek origins, deriving from the Greek word for the "gift of governance" and "leadership." In Pennsylvania, we have been tapping both aspects of the word in our election security planning, using resilient and integrated governance and leadership to enhance the intersections and communications between people and machines, to continue to advance our technologies while also doing so in a way that protects our democracy and develops collaborative and responsive policy and leadership. This requires a tremendous amount of resources but has immeasurable value.

Collaboration

Thanks to Governor Wolf's deep commitment, we have employed a multi-layered and cross-sector security strategy to election security. We broke down silos and brought together experts from multiple fields and sectors at the local, state, and federal levels, including professionals in information technology, law enforcement, homeland security, defense, elections, and emergency preparedness. Beginning in 2018, we formed an executive Interagency Workgroup on Election

Security and Preparedness, banding together experts from the Department of State (DOS), Homeland Security, Emergency Management Agency, Information Technology, State Police, National Guard, the Inspector General, and the Department of Military and Veterans Affairs. This team of key agencies meets regularly and collaborates on increasing election security training, support, assessment, information, and preparedness, to implement best practices to respond to and mitigate continuously evolving security threats.

We also formed a county/state election security workgroup of County Commissioners Association of Pennsylvania (CCAP), county election directors, DOS staff, and county and state CIOs and IT personnel. This workgroup discusses security issues and shares training resources, including guidance, security awareness training, and resources on strong cyber security practices for voting system and network preparation and security, including pre-election testing, password and permissions management, restricting access, file transfers, and vote canvassing. We are also providing anti-phishing and security training tools to all 67 counties at no cost to them.

We have collaborated with all these state and federal partners to provide tabletop exercises to counties and partners, modeled after common military and law enforcement techniques, to train election, information technology, and security personnel in incident response and preparation, simulating scenarios that could impact voting operations.

We were the first state in the nation to accept DHS's offer to provide vulnerability assessments to the states – we did this in 2016, 2018, and are planning a third assessment in the next several months. We have tools in place to identify vulnerabilities, detect network intrusion, and encrypt data in-transit and at rest. We engage in ongoing continuity and disaster recovery exercises and review and revise as necessary our COOP plans several times each year.

Voting System Upgrades and Post-Election Audits

As of 2018, Pennsylvania was one of the small minority of states still primarily voting on paperless Direct Recording Electronic (DRE) voting systems. In April 2018, DOS directed all 67 counties to purchase new voting systems that meet current security and accessibility standards, and which include a voter-verifiable paper record with plain text language that voters can verify before casting their ballot and that local officials can use in recounts and post-election audits. These new systems must be in use no later than by the primary of 2020, and preferably by the November 2019 election.

In order to bolster our voting system security even further, in 2018 DOS created new security standards by which to evaluate the new voting systems applying for certification in PA. PA law requires both federal and state certification, and because the federal EAC had not updated its standards in some time and did not have a quorum to do so at the time, we decided to update our state security standards, and additionally assess the accessibility of the systems. The new voting system standards incorporated tests to ensure confidentiality, vote anonymity, integrity, security, auditability, and usability of the voting systems. All new certified systems in Pennsylvania have passed the following tests:

- Penetration testing that evaluates the security of the voting system by trying to exploit potential vulnerabilities.
- Access control testing to confirm that the voting system can detect and prevent unauthorized access to the system and election data.
- Evaluation of voting system audit logging capabilities to confirm that the system logs will allow auditing, as well as investigation of any apparent fraudulent or malicious activity.
- Tests that ensure every physical access point is well secured and system software and firmware is protected from tampering.

To evaluate accessibility of voting systems for voters with disabilities, we utilized expert review by usability and accessibility examiners as well as feedback from voters with disabilities and poll workers.

DOS has certified seven new voting systems that meet these standards, and we are very pleased with the remarkable progress made by the counties. The county election directors and commissioners have been incredibly dedicated to acquiring voting systems that best meet their voters' needs and provide the most secure, auditable, and accessible voting systems to all Pennsylvanians. Already, 75 percent of counties have officially voted to select new systems, and 46 out of 67 counties are utilizing their new systems with verifiable paper records in November 2019. The remaining counties are still hard at work planning and evaluating their voting system choices, reviewing vendor quotes and prices, holding new voting system demonstrations for the public, consulting with voters and poll workers and exploring funding and financing options.

Cost, of course, remains a major concern for counties. Since the beginning of this initiative, we have been committed to this enterprise being a cost-share of federal, state, and local dollars. Toward this end, we designated 100% of the federal funds appropriated in 2018 for election security proportionately to the counties for replacement of their voting systems by 2020, totaling $14.15 million in PA (including a 5% state match). Though a welcome down payment and approximately 10-12% of the total costs of the new systems, $14.15 million is not nearly enough, and we are pursuing additional state and federal funding.

We have also formed a statewide post-election audit working group, which includes election officials from six counties of different sizes and demographics across the state, as well as expert advisors on audits and elections. This working group is studying audit models such as risk-limiting audits and is developing best practice recommendations for post-election audits that will review the plain text on the paper records and the tabulated votes to confirm to a reasonable degree of statistical certainty the accuracy of the outcome of the election.

The dedication and thorough examination by the members of this workgroup to developing effective models has been inspirational and should be a model for other states looking to explore these practices. In addition, two of our counties on opposite sides of the state, Philadelphia and Mercer county, have volunteered to pilot advanced post-election audits this November 2019,

which will offer confidence to the voters as well as the opportunity to establish and test real-time best practices. Additional Pennsylvania counties will also be piloting audits over the next several years, and we expect all counties to employ enhanced audits by the 2022 general election.

Looking Forward

Looking forward, we continue to build. The above initiatives have taken and will continue to take significant resources to advance. In addition to advancing and strengthening all of the above, our highest priority goals and need for additional resources include: replacing our statewide voter registration system (SURE); ensuring all counties have advanced intrusion detection systems and practices, ongoing and evolving comprehensive cyber hygiene assessments, COOP and security training, and vulnerability assessments; and implementing new voting systems, strengthened pre-election testing, and enhanced post-election audits statewide.

CONCLUSION

On Election Day 2018, we saw what happens when all of the collaboration and hard work comes to fruition, and the powerful benefits of the intersection of all of the above in action. We were connected throughout the day to the counties, state agencies, other states, and the federal government through shared dashboards and frequent communications. For example, if another state was seeing attempted attacks coming from particular IP addresses, they were able to share with other states, allowing us to block those IP addresses at the state level, and then Pennsylvania would share those IP addresses with all 67 counties to enable them to block those IP addresses as well. We had conference calls throughout the day with our interagency group members and counties, sharing what we were hearing and seeing, any concerns, and any support or resolutions we could provide from our different sectors. This collaboration and communication allowed us to be proactive in our defenses, rather than just reactive as might have occurred in the past.

The right to vote is a fundamental right, and every voter must be provided equal access to the polls and deep-seated confidence in the security and accuracy of their vote. We cannot allow circumstances to develop whereby voters in under-resourced counties have less security or less accessibility in their vote. Pennsylvania — where both the Declaration of Independence and the U.S. Constitution were adopted — takes its legacy as the birthplace of American democracy very seriously, and we know that the foundation of that democracy rests on the security, auditability, accessibility and integrity of our elections. We urge you please to invest additional funds to ensure this for ourselves and for generations to come. Our democracy - and bolstering voters' confidence in their ability to participate fully in that democracy - is worth every dollar.

Thank you for the opportunity to testify on this important issue, and I am happy to answer any questions you may have.