TESTIMONY ON PENNSYLVANIA'S CYBER SECURITY AND ELECTIONS

PRESENTED TO THE SENATE STATE GOVERNMENT AND TRANSPORTATION COMMITTEES

Joint Public Hearing to Discuss Motor Voter, Unlawful Voting and Cyber Security

BY

RITA REYNOLDS

CIO

DECEMBER 12, 2017

Good morning. I am Rita Reynolds, CIO for the County Commissioners Association of Pennsylvania. The CCAP is a non-profit, non-partisan association providing legislative, education, research, insurance, technology, and other services on behalf of all of the Commonwealth's 67 counties. In the area of technology, CCAP provides a number of county programs including IT assessments which focus on assisting counties with ensuring their technology infrastructure and support are up to industry standards, IT CORE services where counties have access to resources of standard IT policies, and several statewide aggregate agreements including cyber security educational tools. We also provide forums and other support for county IT professionals and GIS professionals.

Thank you for the opportunity to be here today to discuss Pennsylvania's election system security and the work we are doing in conjunction with the counties and the Department of State to improve cyber security as it pertains to elections. While I am not involved directly in the use or setup of voting equipment, my knowledge comes from the frequent interactions with county CIOs and IT Directors who do provide the setup and support for their election offices, as well as a strong relationship with the Department of State.

I also bring to this hearing my 30 years of expertise in the technology world. Since the term cyber security has begun to be widely used, I have focused a significant portion of my time and efforts around education and creation of programs that increase the technology security posture of county government.

Turning to the topic of today - motor voter, unlawful voting and cybersecurity – counties are responsible for administering and maintaining election duties including the registration of citizens to vote, election activities leading up to and including election day, election results and the purchasing of voting equipment. Counties take pride in securing the most fundamental democratic right of Americans – the ability to vote, and the assurance of free and fair elections.

In many counties, the IT department supports the technology aspects of the elections and voter registration offices. Depending on the county this technology support may include Logic and Accuracy testing, calibration and distribution of the election voting equipment, technical support on the day of an election and transfer of the results at the end of the day. Transfer of the results can range from packaging the data onto a mobile device like a USB drive, or manually carrying machine cartridges or ballots back to the election offices for final processing. From there secure methods are used to send the total aggregated results to the state as well as the posting of unofficial results on the county website. As one should expect, the technical aspects have significantly increased over the years.

History of Cyber Security

In the broadest context, the evolution of technology has brought improvements to how counties conduct all official business. It has also resulted in the rise of security exposures to county systems and data, with electronic data breaches becoming much more prominent since about 2005. These breaches can occur by multiple methods, including:

- Cyber attacks where code is distributed onto servers and computers and destroys files and other data
- Cyber hacking where an individual or organization gains access to servers or computers for the purpose of stealing vital organizational, financial, or citizen data
- Phishing email campaigns where individuals receive fake emails that either contain attachments with code that can adversely affect an entire network or include links to what appear to be valid websites where individuals unknowingly provide confidential information
- Ransomware, where third parties hack in to control servers or software, and extort payments to restore access
- Poor administrative controls and procedures where an unauthorized individual can easily gain either physical or remote access to servers and other devices
- Physical security vulnerabilities of data centers where the technology servers and devices are located. Data centers should contain multiple layers of security from entering the building to the department to the data room to the rack where the server resides

We hear on a regular basis from media reports that another company or government entity has been infiltrated by one of these methods. The Committee members are all aware of major breaches at Target, Yahoo, JP Morgan Chase, Equifax, the US Office of Personnel Management, Home Depot, Amazon Web Services and Adobe. And this list is certainly not exhaustive. The recent announcement of the data breach at the UBER ride sharing company, continues to highlight the extensiveness and severity of this modern day problem – and the sometimes insufficient responses from the holders of data.

On a countywide scale, IT departments have worked hard to utilize emerging technologies and tools to strengthen the county security posture. In technical terms this means at minimum implementing firewalls, server update regimens, spam filters, encryption, and SSL for websites. In layman's terms this means securing your home with a fence, gates with keypads, door locks and fireproof safes for valuables within the home, and then regularly ensuring that maintenance is performed on each of these elements

Further complicating the technology landscape, is the focus that counties must now take on physical security and human resource security. Moving servers to secure, climate controlled, all-hazards protected facilities is a significant capital and operating expense. Likewise, the processes of limiting employee access to only job-related software and files, and training them on sound security practices (especially email, file sharing, and password administration) are time consuming but important. Our interfaces with state databases – SURE is the example before the Committee today, but we also have databases and shared reporting systems with the state across a variety of human services, land use, and other programs – must help us do our jobs but also protect the data we hold. And our next issue is transferring these protocols over to the emerging technology of cloud computing.

Election System Issues

The counties' security defense covers all that happens behind the scenes for every county department, including the election department and related equipment. One of our most

frequent questions is the security of our election equipment, particularly from those who claim that election voting equipment is non-secure and easily hackable. DEFCON, one of the world's largest annual hacker conventions, is a great example where conclusions on the secureness of voting systems were drawn based on tests performed in wholly unrealistic scenarios. This is not to say that valuable lessons cannot be learned from such testing efforts, but we need to keep in mind that the access hackers had at DEFCON does not match the real world: Our election equipment is secured in locked facilities, it is never connected to the internet, it is tested before and after deployment, it is securely transported, and it is monitored during elections.

On the point of physical security, it was common place years ago to store equipment in locations that multiple employees had access to. Lever machines did not require the same type of security now needed for DRE and Optical Scan voting machines. Counties have had to implement stronger chain of custody protocols, including physical room security (with climate control and sometimes cameras or intrusion detection), tighter procedures for who is permitted access to rooms where election equipment is stored.

Current Efforts

County IT staff recognized many years ago that cyber security was going to result in the need for more proactive tools and resources to combat the volatile environment that cybercrime now plays in local government. Locally, counties have implemented changes such as:

- Requiring multiple background checks – initially these were completed on only certain IT staff. Today many counties conduct background and FBI checks on all IT staff and require the same for all vendors entering secure locations and accessing county technology applications.
- Requiring initial and on-going education – While counties are doing a very good job with initial training of acceptable use and access to technology systems, on-going education has proven to be more challenging. To this end CCAP is working with county IT departments to provide a statewide standard framework for dealing with security issues, both generally as well as with election offices.
- The creation of Pa CyberSafe – Arising out of a 2015 CCAP initiative with county CIOs, we have created Pa CyberSafe. The group meets on a quarterly basis and has successfully implemented a number of vital cyber security initiatives including an annual cyber security conference, a self-assessment security toolkit (which six counties have completed), and the encouragement for all counties to participate with the Multi-State Information and Sharing Analysis Center (MS-ISAC) to have vulnerability scanning completed on a regular basis for all of their externally facing websites and related applications.
- State Partnerships – In late 2016, CCAP partnered with the state Office of Administration on procuring phishing software that has allowed counties to conduct random email testing for employees using real-life scenarios. The renewal of this program now includes a learning management system that provides online educational tools for employees to use to raise their cyber awareness.
- Cyber Insurance – As with physical structures and other equipment, counties recognize that insurance is becoming a necessity for cyber incidents, and this insurance mandates loss control efforts that improve security in its own right.

- IT Assessments – CCAP has been performing onsite IT assessments since 2010, which are designed to be an independent, third party, non-vendor review conducted by CCAP Technology staff. The process includes interviews of key departments covering general and specific questions related towards evaluating and assessing the current technology environment and needs of the county. Throughout the assessment, questions are geared towards security, to help build security recommendations into the Executive Summary.

Relating to voting and elections technology, most recently, Pa CyberSafe is now partnering with the Department of State on developing a county inventory and validating industry standard approaches with counties on networking infrastructure that meets voting system requirements. Other work to be finalized in the next several months includes the development of standardized security policies and incident procedures.

As to voting equipment, it is important to recognize that technologies are advancing which facilitate higher degrees of security and which afford voters with greater confidence in the equipment and the results. That pairs with the realization that all of the equipment in the Commonwealth is at least ten years old, coming up rapidly against its anticipated useful life. In this respect, we will need state assistance, first to achieve Department of State certification for next generation election systems, and second to find available funding to perform upgrades. For perspective, when we did statewide replacement of election systems in response to Help America Vote Act (HAVA) requirements, the price tag was $100 million – and that did not include Philadelphia and Dauphin counties.

Recent Legislation

Due to the rise in cyber security incidents, there are national and statewide legislative efforts to implement tighter controls around the notification of breaches. CCAP and state agencies are working together closely to fine tune proposed cyber security legislation. Areas that we are working collaboratively on include improving security definitions, improving levels of reporting and notification timeframes, and including tighter controls and standards for the vendor community which supports county functions, including election services.

In the Near Future

While counties want to see and support tighter legislation, this will result in increased costs to local government. The newly formed partnership with the Office of Administration and Technology and the Department of State are critical to ensuring that these initiatives continue and grow and that all counties are able to afford these same efforts. It is important to recognize that all of these system-wide cyber security efforts also tie directly into supporting the county election offices and their work. As new election voting equipment is explored there will be technology impacts, especially if there are voter verifiable ballot components. As a result, stronger data security measures will be needed, which will come at a significant cost.

We appreciate the partnership we have had to date with the Office of Administration/ Information Technology and the Department of State, and we stand ready to continue and

expand that partnership as may be necessary in determining the future direction of the SURE system and new election equipment.

Thank you for your attention to these comments, and I will be pleased to answer your questions.