TESTIMONY ON
CYBERSECURITY FOR CLOUD-BASED GOVERNMENT APPLICATIONS

Presented to the Pennsylvania Senate Communications and Technology Committee

By
Michael Sage, CCAP, Chief Operations and Information Officer
Justin Loose, County of Berks, Chief Information Officer

March 13, 2023

Michael Sage, CCAP Chief Operations and Information Officer

On behalf of the County Commissioners Association of Pennsylvania (CCAP), representing all 67 counties in the commonwealth, I write to share our comments on cybersecurity for cloud-based government applications.

Counties take seriously their responsibility to protect personal information and the critical services that they offer and administer, by implementing the best possible cybersecurity standards and practices. County technology leaders and executives actively participate in a wide range of cybersecurity education and awareness activities and groups. These range from local and state groups, like CCAP, to national groups like the Multi-State Information Sharing and Analysis Center (MS-ISAC) and others. By keeping up to date with trends, threats, best practices, and general awareness, counties are positioning themselves to protect their information and critical systems from cyber threats, and developing processes to respond if or when a cybersecurity incident happens.

As the technology world continues to change and more and more information services and applications move to the cloud, staying up to date on best practices and threats is vital for counties. Many counties are exploring the use of cloud-based services and applications, by taking a use case model approach towards the use of the cloud, and not just blindly jumping into the cloud. Working across county departments to ensure both business and cybersecurity requirements are being met is quickly becoming the norm across all counties.

Counties are developing internal processes to evaluate cloud-based services and applications to ensure they comply with the county's requirements and with national standards. The cloud industry has come a long way over the last couple of years. More and more providers are able to meet national standards like FedRAMP and others. These national standards and certifications are great, but counties are working to ensure any cloud provider they may leverage has the security protocols and resources in place to comply with current security best practices and standards. Security doesn't stop with the cloud service provider; it extends to the county's network. This is why counties are continuing to assess and strengthen their cybersecurity posture.

As with anything, end users can be the weakest point in any cybersecurity strategy, and this includes usage of cloud-based services. That is why counties continue to develop, exercise, and educate county employees on good cybersecurity practices and behaviors.

Due to the rise in cybersecurity threats CCAP, counties, other local government organizations, and state agencies are already working together closely to improve security definitions and implement vital cybersecurity initiatives, conducting reoccurring quarterly meetings, an annual cybersecurity conference, security resources and other projects. Our partnership has also extended to federal partners as well. Counties take extensive care to remediate any incident that may occur, and actively work to mitigate threats to prevent an incident from occurring in the first place. CCAP's collaboration with the Office of Administration (OA) to enable counties to

leverage cost-effective security awareness training and anti-phishing exercise capabilities that allow for additional education at a shared cost. CCAP has also worked with the Department of State (DOS) to identify short term funding for intrusion detection systems for county election infrastructure. CCAP, OA and DOS communicate regularly in an effort to expand and identify new areas of collaboration and coordination to improve the overall cybersecurity posture of counties and the commonwealth.

While these intergovernmental partnerships have proven invaluable, we would also support the establishment of a state Cybersecurity Coordination Board, to help coordinate cybersecurity matters across all levels of government in the commonwealth and the private sector. Additionally, while CCAP has been working closely with a number of state agencies on the federal State and Local Cybersecurity Grant Program these funds are slated to be spread across all local government entities and schools, diluting the funding. Plus, these funds are only available through 2026. To help counties to continue to address cybersecurity threats and implement security best practices in the long-term, counties are seeking a re-occurring state budget line item to enable counties to continue to address and adapt to cybersecurity protocols and best practices as the technology field continues to change and grow.

Counties take seriously their responsibility to protect information and want to implement the best possible cybersecurity standards and appreciate the opportunity to have representation on the board for the grant program. Counties value the close working relationship between the state and counties to ensure the county voice is heard in IT decisions and best practices can be shared.

Thank you for your consideration of our comments. Please contact us if you have questions or need additional information.

Justin Loose, County of Berks, Chief Information Officer

I am honored to have the opportunity to submit comments regarding cybersecurity and cloud-based applications on behalf of Berks County.

Cybersecurity, including its component aspects of data availability, data integrity and data confidentiality are, collectively, a top priority for Berks County. Cybersecurity needs have driven most of our IT related projects and, subsequently, most of our IT budget for the last several years. There is no sign that this trend is decreasing. Cybersecurity needs have increased the pace of our technology deployment as we race to upgrade or replace systems to ensure that they can accept the most recent patches and updates needed to keep pace in today's cybersecurity landscape. Cybersecurity needs have necessitated undertaking application modernization to ensure that we have systems capable of safeguarding the data of our residents and our employees.

Most new IT projects result in the implementation of technology that is either fully cloud-based,

or a hybrid of cloud-based and on-premise technology. In many cases, we are being compelled into the cloud by our vendors, either because the vendor no longer supports any on-premise products, or because new required or desirable features are only available in the cloud versions of their products. As such, Berks County currently uses several different cloud technologies. The county has a few cloud-based "Software As A Service (SAAS)" applications. These applications require us to accept both security and feature updates based on a schedule defined by the vendor.

The cloud applications provide several benefits. It allows us to reduce on-premise technology and provides us with beneficial features for disaster recovery. It also, generally, provides us with robust tools for security and patching. While we benefit from the timely access to security updates, the staff input for testing security and feature updates does not change. It also becomes difficult to understand the security or confidentiality implications of feature changes. The prevalence of SAAS applications means that we have applications in multiple cloud providers. This multi-tenancy creates a challenge for the County in that we must deal with many different vendors, each with different schedules for updates and enhancements, and many different management interfaces.

With cloud technology, the County lacks visibility into a vendor's cyber security posture. We cannot see if their employees are following cybersecurity best practices. We are forced to rely on our vendors to ensure our data is secure. We must rely upon negotiated contractual terms for us to manage this vendor risk. Negotiating the required controls for cybersecurity into an IT contract is no easy task. Berks County is a third-class county and counties our size and smaller have limited bargaining power and limited ability to dictate terms with larger vendors. This creates additional pressure on a procurement process that is already complex. Continued work by the federal and state governments to develop standards for security, such as FedRAMP, are helpful and welcomed, but ultimately the work necessary to ensure that vendors are meeting compliance for security and confidentiality continues to fall on the County. I would ask this committee for its help in ensuring that we collectively identify better avenues to find creative ways to work with our vendors to ensure that they have appropriate incentives to maintain the security and privacy of their client's data and ensure that they can be held accountable for failures.

There is no doubt that cybersecurity and cloud technologies are forcing a growth in IT expenditures in our county. Our spending in cybersecurity technologies has more than quadrupled over the last four years, and this trend also shows no sign of decreasing. In many cases, technology expenditures related to the cloud technology and cybersecurity have switched from capital costs every three to five years with smaller annual support payment to larger subscription based operational expenses. Ultimately it all costs more. The price of cyber liability insurance continues to increase despite ongoing efforts and expenditures to meet the demands of the insurance industry. While the cloud offers solutions to some cybersecurity challenges, it

creates others.

Elections security has also been a focus for Berks County. We are committed to safe and secure elections. We understand that ensuring we have a secure election means that we have to take a holistic approach to security with our networks, our server assets, our workstations and, most importantly, our employees. Collaboration is a key aspect of security. Counties rely upon collaboration with the commonwealth, through the Office of Administration; collaboration with other counties, through CCAP, and collaboration with other partners such as the National Guard and the Multi-State Information Sharing and Analysis Center (MS-ISAC) for technical resources. Effective and efficient cybersecurity requires that this collaboration continues to expand.

Counties like Berks will continue to need fiscal support from the state to continue to safeguard the data of our constituents. To be effective, these funds should be dedicated to cybersecurity and annually appropriated to ensure service continuity and supports. The federal funding provided by the State and local Cybersecurity Grant Program is a great start, but we will need to establish long term funding solutions that will ensure that all counties, municipalities, schools and health systems have the funding they need to provide adequate security.

I would like to thank you again for the opportunity to submit these comments. I am happy to address any additional questions.