TESTIMONY ON
CYBERSECURITY ISSUES FOR LOCAL GOVERNMENTS

Presented to the Senate Local Government and Communications and Technology Committees

By
Joe Sassano, Executive Director of IT and Chief Information Officer, York County

January 31, 2024

I am Joe Sassano, Executive Director of IT and Chief Information Officer for York County, and I appreciate the opportunity to offer remarks today on cybersecurity for local governments. I also serve as a member of the Technology Committee, a standing policy committee of the County Commissioners Association of Pennsylvania (CCAP). CCAP is a non-profit, non-partisan association representing the commonwealth's 67 counties.

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.

Counties provided testimony earlier this legislative session on cloud-based applications for government use and some of the cybersecurity concerns and best practices that go along with that shift in technology. Many of those themes still apply, noting that as the technology world continues to change and more and more information services and applications move to the digital platforms, staying up to date on best practices and threats is vital for counties.

Cybersecurity, including its component aspects of data availability, data integrity and data confidentiality are, collectively, a top priority for counties. Counties are continuing to assess and strengthen their cybersecurity posture. Working across county departments to ensure both business and cybersecurity requirements are being met is quickly becoming the norm across all counties. As with anything, end users can be the weakest point in any cybersecurity strategy. That is why counties continue to develop, exercise, and educate county employees on good cybersecurity practices and behaviors.

In York 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.

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 tripled over the last four years, and this trend also shows no sign of decreasing. The budget increases have been to address the evolving threat landscape as counties purchase and implement tools to mitigate the cybersecurity risks. There have been other commonwealth policy changes, such as Act 151, Breach of Personal Information Notification Act, FBI changes for accessing and

processing of CJIS data, which have added to county budgets. Additionally, the price of cyber liability insurance continues to increase despite ongoing efforts and expenditures to meet the demands of the insurance industry. Further, counties and local governments are going to be dealing with the rise in Artificial Intelligence (AI), which will require additional defenses and considerations to ensure information and systems are secure and protected.

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, counties 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. These programs only address a small piece of the required funding and are only good for a couple of years, several ending in 2026. Longer term and increasing funding to support county cybersecurity is needed. To help counties to continue to address current and evolving 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 are requesting $2.5 million in the 2024-2025 state budget for county cybersecurity programs as a way to build sustainable funding to protect Pennsylvania's valuable systems, assets and information.

Equally spreading the $2.5 million among the 67 counties would allow for roughly $37,000 per county ($17,000 for Albert Sensors and $20,000 for other county cybersecurity initiatives). However, the funding should not be prescribed by that breakdown as the county would be best fit to determine how to allocate the $37,000 each year based on their local needs and other grant funding opportunities. For example, the IIJA cybersecurity grant requires a fund match, for year one the state covered the match (10%). It's undetermined if the state will cover the year two 20% match or if that will come down to counties to cover. This 20% match could be a real sticking point for counties, and this cyber funding ask would go a long way to helping counties.

Additionally, counties would benefit from an increase in funding for the Pennsylvania National Guard (PANG) to help counties with cyber assessments and response ($500,000 to $1,000,000). Over the last couple of years, the PANG has been able to assist counties by performing cybersecurity assessments in an effort to identify areas that counties can strengthen to better protect themselves and the critical services and data they maintain. However, the efforts by the PANG have been limited due to funding, as their cybersecurity services are completely funded with federal dollars today. Counties value the working relationship between PANG and counties, and the counties are interested in opportunities that would enable the PANG to expand and better serve counties related to cybersecurity.

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 current cybersecurity 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.

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