CCAP
COUNTY COMMISSIONERS
Association of Pennsylvania

TESTIMONY ON
CYBERSECURITY ISSUES FOR LOCAL GOVERNMENTS

Presented to the House Local Government and Communications and Technology Committees

By
Commissioner Dave Glass
Clearfield County

February 25, 2026

Thank you, Chairman Ciresi, Chairman Ortitay, Chairman Freeman, Chairman Miller, and members of the House Local Government and House Communications and Technology Committees for the opportunity to testify before you today. My name is Dave Glass, and I serve as a County Commissioner in Clearfield County and as First Vice President 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 they deliver and administer by implementing strong cybersecurity standards and practices. County technology leaders and executives actively participate in a wide range of cybersecurity education and awareness initiatives. These efforts range from local and state groups, such as CCAP, to national organizations like the Multi-State Information Sharing and Analysis Center (MS-ISAC). By staying up to date on trends, threats, and best practices, counties are positioning themselves to safeguard critical systems and sensitive information while also developing robust response processes for cybersecurity incidents when they occur.

In recent years, Pennsylvania counties have experienced a range of significant cybersecurity incidents that underscore the persistent and evolving threat landscape. Several counties have faced ransomware attacks and system breaches that disrupted critical services, temporarily took systems offline, and required extensive remediation efforts. In some cases, unauthorized access to sensitive resident data occurred, triggering costly notification, legal, and recovery processes. Emergency communications systems have also been impacted by cyber incidents, requiring manual operations until systems could be restored. These examples illustrate the real and ongoing cyber threats facing counties across the Commonwealth and the substantial operational and financial resources required to respond and recover.

Counties have provided testimony in prior legislative sessions on cybersecurity, including the growing use of cloud-based applications in government and the associated risks and best practices. The same general themes continue to apply: as technology evolves and more information services and applications move to digital platforms, maintaining current cybersecurity practices and threat awareness is essential.

Cybersecurity—including the foundational principles of data availability, data integrity, and data confidentiality—is a top priority for counties. Counties continuously assess and strengthen their cybersecurity posture. Collaboration across departments to ensure that both operational and security requirements are met is standard practice. As with any organization, end users can represent a point of vulnerability. For that reason, counties continue to invest in training, exercises, and employee education to promote sound cybersecurity behaviors.

In many counties, cybersecurity demands have driven numerous IT-related projects and have consumed a significant share of county IT budgets in recent years. There is no indication that this trend will slow. Counties are accelerating system upgrades and replacements to ensure compatibility with current security patches and updates. Cybersecurity needs have also required application modernization so counties can better safeguard the data of residents and employees.

There is no doubt that cybersecurity and cloud technologies are contributing to increased IT expenditures across all counties. Budget increases are largely driven by the evolving threat landscape, requiring counties to purchase and implement tools to mitigate cybersecurity risks.

In addition, recent Commonwealth policy changes—including Act 151, the Breach of Personal Information Notification Act, and FBI requirements related to Criminal Justice Information Services (CJIS) data—have added to county costs. The price of cyber liability insurance continues to rise despite counties' substantial investments to meet underwriting standards. Further, counties are increasingly addressing the rise of Artificial Intelligence (AI), which requires additional safeguards to ensure systems and data remain secure.

Counties have also experienced added security responsibilities and costs associated with cloud-based infrastructure. Most new IT projects now involve either fully cloud-based systems or hybrid models combining cloud and on-premise technologies. In many instances, vendors are phasing out on-premise products or limiting new features to cloud platforms, effectively compelling counties to migrate. While cloud solutions offer benefits, they also raise important questions about vendor cybersecurity posture. Although vendor security practices are not directly within county control, counties must rely on vendors to protect the sensitive data entrusted to them.

Counties maintain particularly sensitive information, including court records, deeds and property data, human services files, election records, and emergency services systems. These systems are prime targets for cyber threats, as demonstrated by prior incidents. Technology improves efficiency but also expands the surface area for potential vulnerability.

Election administration presents a uniquely heightened cybersecurity challenge because county governments operate critical election infrastructure that must be consistently available, accurate, and secure. In recent election cycles, county election systems have faced extremely high volumes of attempted cyber intrusions, many originating from foreign actors, as well as coordinated disruption efforts such as targeted bomb threats directed at election facilities. While counties have successfully defended against these threats, such incidents place extraordinary strain on local IT staff, election administrators, and emergency response personnel. Even unsuccessful attempts can impact public confidence, require expanded security measures, and increase operational costs. The protection of election systems is therefore not only a technical responsibility but a matter of public trust and democratic stability.

Cybersecurity has also been identified as a significant cost driver within county 911 systems and contributes to counties' priority request for an increase in the 911 surcharge. Although this testimony is not directly tied to a specific state appropriation request, counties respectfully urge the General Assembly to strongly consider raising the 911 surcharge to $2.20, in part to help cover the growing costs of securing this critical, life-saving service.

In response to rising cybersecurity threats, CCAP, counties, other local government organizations, and state agencies are working collaboratively to strengthen cybersecurity coordination. These efforts include recurring quarterly meetings, an annual cybersecurity conference, shared security resources, and additional joint initiatives. Our partnerships extend to federal entities as well. Counties take swift and comprehensive action to remediate incidents when they occur and work proactively to prevent them.

CCAP has collaborated with the Office of Administration to allow counties to leverage cost-effective security awareness training and anti-phishing exercises through shared purchasing arrangements. CCAP has also partnered with the Department of State to identify short-term funding for intrusion detection systems supporting county election infrastructure. CCAP, the Office of Administration, and the Department of State communicate regularly to identify additional areas for coordination and to strengthen the cybersecurity posture of counties and the Commonwealth.

While these intergovernmental partnerships are invaluable, counties also support the establishment of a State Cybersecurity Coordination Board to improve coordination across all levels of government and with the private sector. Although CCAP has worked closely with state agencies on implementation of the federal State and Local Cybersecurity Grant Program, those funds were distributed across all local governments and school districts and were insufficient to meet the overall need. These programs addressed only a portion of required funding, and several are set to sunset in 2026. With Infrastructure Investment and Jobs Act funding concluding, long-term and sustainable cybersecurity funding is essential.

To ensure counties can address both current and evolving cybersecurity threats, counties urge the Commonwealth to establish a sustained, coordinated investment in county cybersecurity. This investment should include:

- Ensuring all 67 counties retain membership in the Multi-State Information Sharing and Analysis Center, preserving access to threat intelligence, vulnerability scanning, incident response, and training;
- Providing flexible, recurring funding for tools such as Albert sensors, endpoint protection, backup systems, cybersecurity training, and other evolving local needs;
- Supporting the creation and staffing of a Statewide Cybersecurity Coordination Committee to develop a shared governance model, define service priorities, and manage a shared-services program offering vetted cybersecurity tools at discounted rates;
- Delivering voluntary cybersecurity assessments to help local governments evaluate risk posture and target resources effectively; and
- Expanding the Pennsylvania National Guard’s capacity to perform cyber assessments, assist with incident response, and conduct resilience exercises with local IT teams.

While counties are not presenting a specific mandated dollar request, a recurring state budget line item dedicated to county cybersecurity would allow counties to continue adapting to evolving threats and best practices. Even a modest investment of $2.5 million in the 2026–2027 state budget would represent an important first step toward sustainable funding to protect Pennsylvania’s critical systems, assets, and information.

If evenly distributed, $2.5 million would provide approximately $37,000 per county. However, funding should remain flexible so each county can allocate resources based on its unique risk profile and available grant opportunities.

Counties would also benefit from increased funding for the Pennsylvania National Guard to expand cyber assessment and response capabilities. In recent years, the Pennsylvania National Guard has conducted cybersecurity assessments to help counties identify vulnerabilities and strengthen defenses. However, these efforts are constrained by funding and capacity. As of November 2025, the National Guard had completed more than 60 cybersecurity assessments across state agencies, counties, municipalities, and school districts, with additional assessments scheduled and a growing waitlist of requests. Counties greatly value this partnership and support efforts to expand the Guard's ability to serve local governments.

Counties take seriously their responsibility to protect sensitive information and are committed to implementing strong cybersecurity standards. We appreciate the opportunity to have county representation on the current cybersecurity grant program board and value the strong working relationship between state and county partners to ensure local voices are heard and best practices are shared.

Thank you again for the opportunity to provide this testimony. I am happy to answer any questions.