House Communications & Technology Committee &

House Local Government Committee

Meeting Agenda

Wednesday, February 25, 2026
1:00 pm
523 Irvis Office Building

1:00pm **Call to Order**

Roll Call

Opening Remarks

1:10pm **Panel 1:** Cybersecurity Experts

- Randy Trzeciak; Director, Masters of Science Information Security Policy & Management (MSISPM) Program; Deputy Director, Cyber Risk and Resilience, Software Engineering Institute, CERT Division; Carnegie Mellon University
- Heather Morton; Director, Financial Services, Technology and Communications, National Conference of State Legislatures (NCSL)

1:40pm **Panel 2:** Cybersecurity Providers

- Thomas MacLellan, Director, Government Affairs & Strategy, Palo Alto Networks
- Dr. Justin Davis, Director of Cybersecurity Integration and Innovation, Unisys

2:10pm **Panel 3:** Local Government

- Dave Glass; Clearfield County Commissioner; 1st Vice President, County Commissioners Association of PA (CCAP)
- Craig Fahnestock, Deputy Executive Director of Member Services, Pennsylvania Municipal Authorities Association (PMAA)
- Holly Fishel, Policy & Research Director, Pennsylvania State Association of Township Supervisors (PSATS)
- Kevin Busher, Chief Advocacy Officer, Pennsylvania School Boards Association (PSBA)

2:55pm **Closing Remarks**

3:00pm **Adjournment**

Government Cybersecurity State Legislative Trends

Communications & Technology Committee and Local Government Committee
House of Representatives
Pennsylvania General Assembly
Feb. 25, 2026

STRENGTHENING THE LEGISLATIVE INSTITUTION

HOW NCSL STRENGTHENS LEGISLATURES

Policy Research

NCSL provides trusted, nonpartisan policy research and analysis

Connections

NCSL links legislators and staff with each other and with experts

Training

NCSL delivers training tailored specifically for legislators and staff

State Voice in D.C.

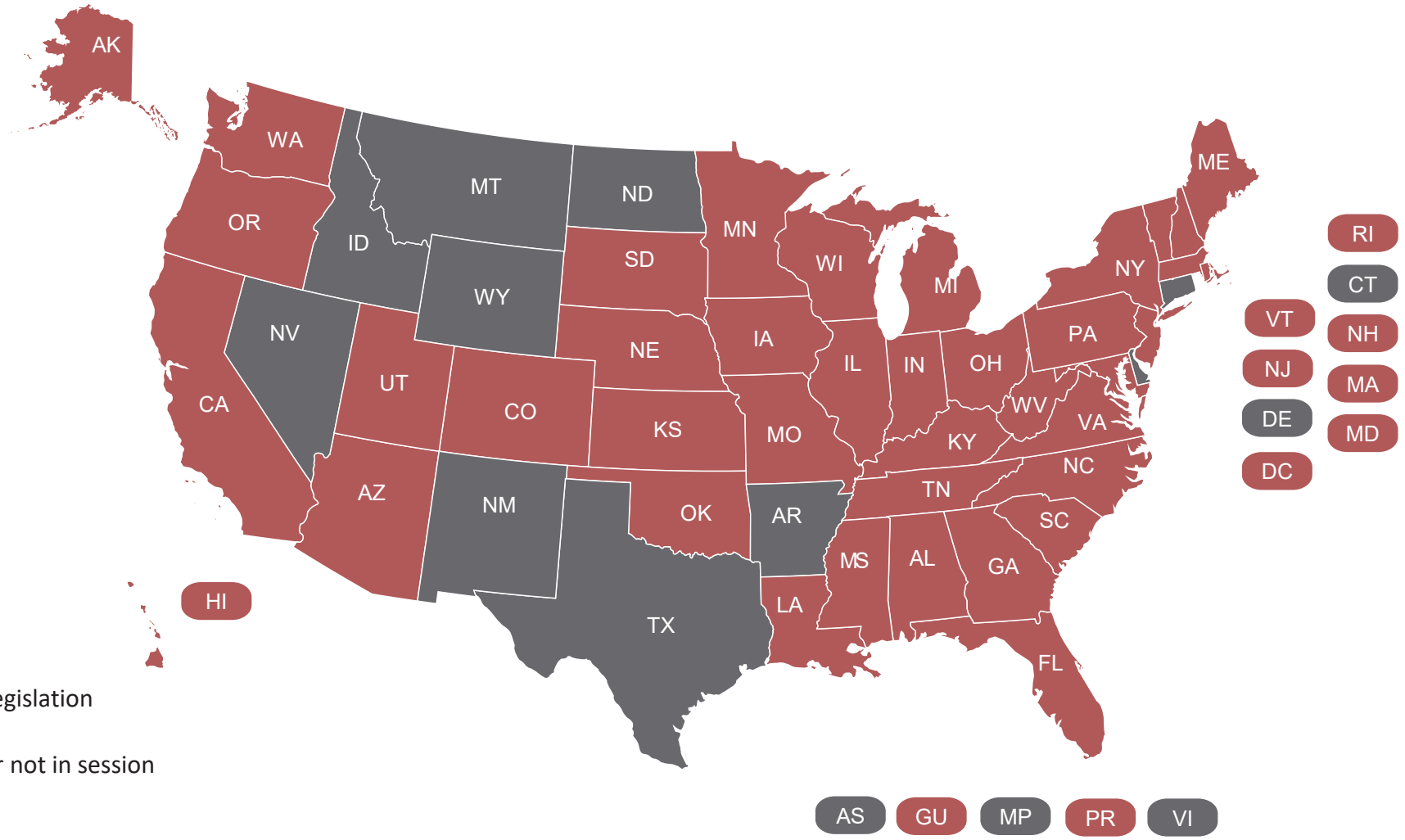
NCSL represents and advocates on behalf of states on Capitol Hill

Meetings

NCSL meetings facilitate information exchange and policy discussions

CYBERSECURITY STATE LEGISLATION

Pending in the 2026 Legislative Session Year



Pending Cybersecurity Legislation

No pending legislation or not in session

GOVERNMENT CYBERSECURITY

Legislation Categories and Topics

- **Cybersecurity Practices for Governmental Entities**
  - Cyber Incident Reporting
  - Limits on sharing information through public records
  - Encryption
  - Multifactor Authentication
- **Critical Infrastructure Protections and Requirements**
- **Technology from Foreign Countries**
- **Civilian Cyber Corps**

ADDITIONAL NCSL RESOURCES

Historical Legislation Tracking

- Cybersecurity Legislation 2025
- Cybersecurity Legislation 2024
- Cybersecurity Legislation 2023
- Cybersecurity Legislation 2022
- Cybersecurity Legislation 2021
- Cybersecurity Legislation 2020

FEDERAL LEGISLATION

119th Congress

- The State and Local Cybersecurity Grant Program has been reauthorized through Sept. 30, 2026, but with DHS in a partial shutdown no new funding is flowing.
- H.R. 5078, Protecting Information by Local Leaders for Agency Resilience (PILLAR) Act
  - Extends SLCGP through 2033 but contains no dedicated funding mechanism.
  - Passed House Nov. 2025
- S.3251, State and Local Cybersecurity Grant Program Reauthorization Act
  - Reauthorizes SLCGP.
  - Introduced Nov. 2025
- White House Cybersecurity Strategy – soon to be released.


NCSL LEGISLATIVE
SUMMIT
CHICAGO
JULY 27-29 | 2026

STAY CONNECTED

- Learn about NCSL training.
- Subscribe to policy newsletters.
- Read State Legislatures News.
- Listen to an NCSL podcast.
- Watch recorded policy webinars and training sessions.
- Attend an event.
- Follow @NCSLorg on social media.

Thank you for joining today!

Heather Morton

Director, Financial Services,
Technology & Communications

heather.morton@ncsl.org

303.856.1475

www.ncsl.org

@NCSLorg

Denver
7700 East First Place,
Denver CO 80230

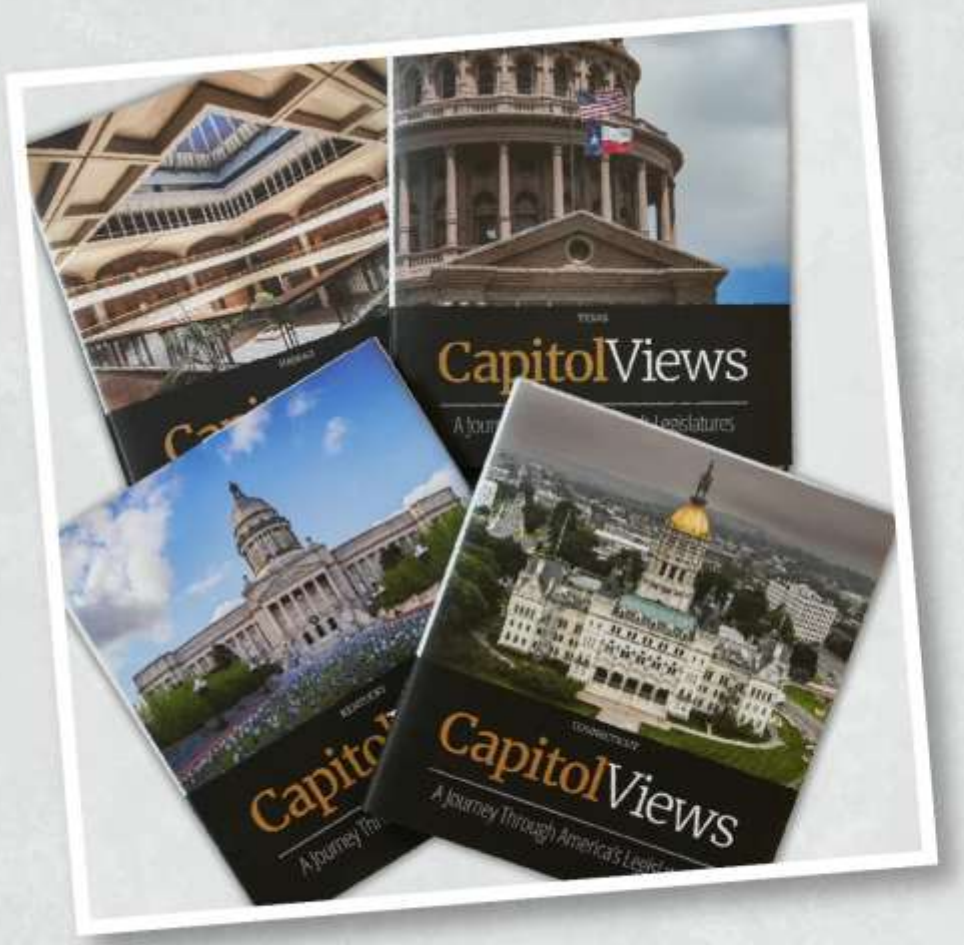
Washington D.C.
444 North Capitol Street, N.W.
Suite 515,
Washington, D.C. 20001

Capitol Views

A Journey Through America's Legislatures

Order Your Customized Edition of **Capitol Views**.

$60 Includes Shipping and Handling.



The National Conference of State Legislatures celebrates its 50th anniversary with a visual exploration of the architectural splendor and historical significance of state capitol buildings across the United States and its territories.

Palo Alto Networks

Presentation to the Pennsylvania House Communications & Technology Committee:
Establishing a Whole of State Cybersecurity Ecosystem

Thomas MacLellan
Director, Government Affairs

OUR MISSION

The cybersecurity partner of choice, protecting our digital way of life.

15K+ Employees | 75K+ Customers Globally | ~$100B Market Cap

9 of 10
of the Fortune 100

8 of 10
Largest U.S. Banks

10 of 10
Largest Utilities in the World

6 of 10
Largest Oil & Gas in the World

8 of 10
Largest Manufacturing Companies in the World

7 of 10
Top U.S. Hospitals

Palo Alto Networks Is a Proven Leader Across Our Platforms

Zero Trust Network Security

Best-in-class Zero Trust Platform across Hardware, Software & SaaS

NGFW
Gartner Magic Quadrant for Network Firewalls

SASE
Gartner Magic Quadrant for Single Vendor SASE

SSE
Gartner Magic Quadrant for Security Services Edge

SD-WAN
Gartner Magic Quadrant for SD-WAN

ZTNA
Forrester ZTNA New Wave

Zero Trust Platform
Forrester Zero Trust Platform Providers Wave

Browser Security
Frost Radar for Zero Trust Browser Security

OT Security
Forrester OT Security Solutions Wave

Internet of Medical Things
Frost & Sullivan Radar for Healthcare IoMT

End-to-End Security Operations

#1 AI-Driven SecOps platform, from code to cloud to SOC

SIEM
Omdia Universe for Next-Generation SIEM
Frost Radar for Modern SIEM
GigaOm Radar for Autonomous SOC

EPP
Gartner Magic Quadrant for EPP
Forrester XDR Wave

SOAR
GigaOm Radar for SOAR
KuppingerCole Compass for SOAR

IR & Managed Services
Forrester Cybersecurity IR Services Wave
IDC Worldwide IR MarketScape
Frost & Sullivan Radar for MDR

CNAPP
IDC MarketScape for CNAPP
Frost & Sullivan Radar for CNAPP
GigaOm CNAPP Radar

Cloud Posture
KuppingerCole CSPM
GigaOm CSPM Radar
KuppingerCole CIEM

Cloud Runtime Security
GigaOm App & API Security Radar
Frost & Sullivan Cloud Application Runtime Security

AppSec
Frost & Sullivan ASPM Radar
GigaOm Radar for Policy as Code
GigaOm Radar for Software Supply Chain Security

Identity Security

#1 Identity Security platform to secure all identities

PAM
Gartner Magic Quadrant for Privileged Access Management

PIM
Forrester Wave: Privileged Identity Management Solutions

Identity Security
Marketscape: Worldwide Integrated Solutions for Identity Security

Identity Platform
Forrester Wave; Workforce Identity Platform

PAM
KuppingerCole Leadership Compass: Privileged Access Management

Identity Fabrics
KuppingerCole Leadership Compass: Identity Fabrics

PAM
KuppingerCole Leadership Compass: Access Management

Secrets Mgmt
KuppingerCole Leadership Compass: Enterprise Secrets Management

ITDR
KuppingerCole Leadership Compass: Identity Threat Detection & Response (ITDR)

We will continue innovating to extend our industry leadership position

paloalto NETWORKS

The world is undergoing rapid digital transformation

AI, Cloud, and automation are reshaping industries.

Artificial Intelligence

94%

of businesses are investing in data readiness for AI

72%

Organizations integrated AI into at least 1 business function

80%

Enterprises are expected to have deployed AI-enabled applications

DATA GROWTH EXPLOSION:

Global data creation is expected to exceed **180 zettabytes**.

Cloud

23%

Increase in Global cloud infrastructure service spending

75%

Organizations will adopt digital transformation with Cloud as primary platform

90%

Organizations will adopt a hybrid cloud approach

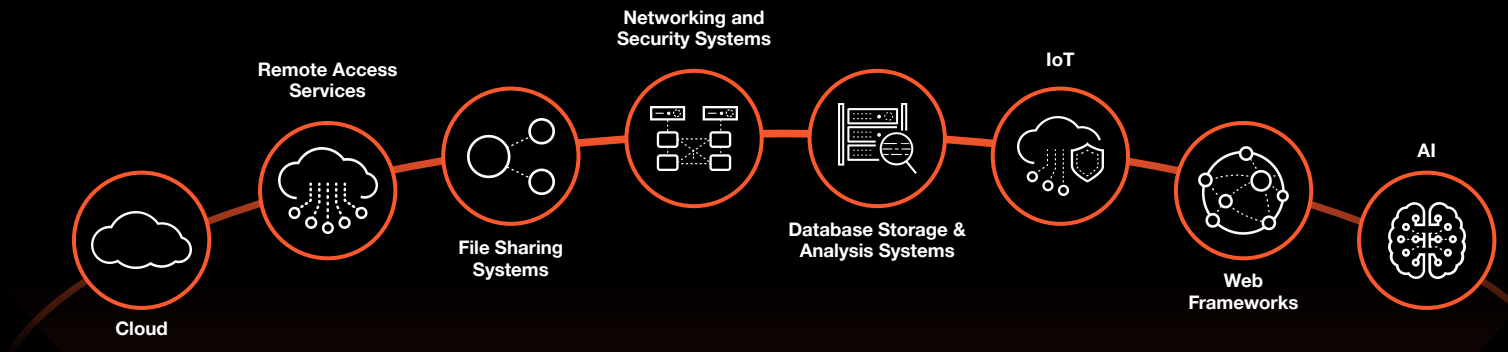
paloalto NETWORKS

AI is supercharging the speed and scale of attacks

Traditional Security Was Not Designed to Keep Up With AI Attacks

Sources: (1) 56% increase in exploited Zero Days in 2023 (Year-on-Year increase based on Google Cloud Blog March 26 2024), (2) 73% increase in Ransomware attacks in 2023 (SANS Blog Jan 15 2024), (3) 78% increase in data breaches and leaks in 2023 (WSJ Article March 15 2024), Most companies need >2-3 days to resolve an incident (XSIAM customer interviews and XSIAM product telemetry for customers)

AI, cloud, and IoT expanded and fragmented your attack surface



Cloud-Related Challenges

1. Data Breaches in Multi-Tenant Environments
2. Complexity of Cloud Security
3. Supply Chain Vulnerabilities

AI-Related Challenges

1. AI-Powered Cyberattacks
2. Adversarial Attacks
3. Bias and Data Privacy

And it's secured by legions of disconnected tools

Quantum computing is arriving sooner than you think

White House Signs Post-Quantum Cybersecurity Guidelines Into Law

- OMB required to “prioritize” switchover to PQC within a year of NIST’s new guidelines
- Nov 18, 2022 OMB issued memorandum for agencies to run audit of QC vulnerable systems

NATO releases first ever quantum strategy

- Strategic ambition of becoming a quantum-ready Alliance includes development of a secure, resilient, competitive quantum ecosystem

Funding Cuts Threaten Security

01 Significant federal funding cuts increase state cyber risks.

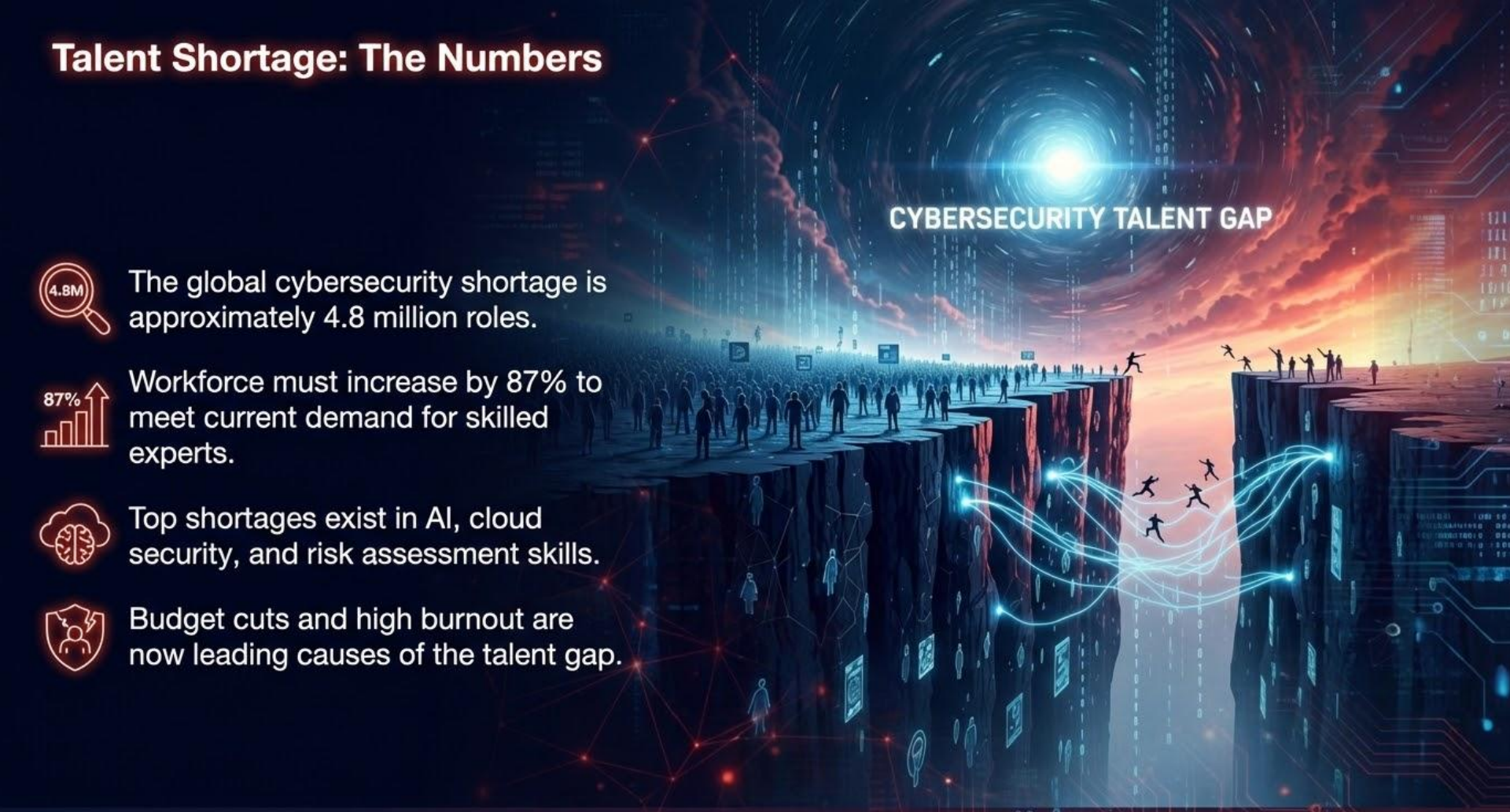
02 State and local systems become more vulnerable to sophisticated attacks.

03 Reduced budgets slow down essential security modernization projects.

04 Cuts impact local government's ability to hire and train staff.

Talent Shortage: The Numbers

- The global cybersecurity shortage is approximately 4.8 million roles.
- Workforce must increase by 87% to meet current demand for skilled experts.
- Top shortages exist in AI, cloud security, and risk assessment skills.
- Budget cuts and high burnout are now leading causes of the talent gap.



What is required to make security work?

From

Fragmented portfolio

Manual operations

Reactive

To

Integrated best in class

Real time AI-driven automation

Proactive

Recommendation: Have a Statewide Incident Response Retainer in Place.

- State-level management enhances local security posture
- Centralized oversight reduces municipal attack surface
- Integrated approach identifies and addresses shared risks
- Proactive strategy protects diverse government systems

Recommendation: Deploy Statewide Attack Surface Management Capabilities.

- State-level management enhances local security posture
- Centralized oversight reduces municipal attack surface
- Integrated approach identifies and addresses shared risks
- Proactive strategy protects diverse government systems

Recommendation: Establish a Joint Security Operations Center.

Centralized Visibility: Real-time threat monitoring across all state and local entities.

Coordinated Response: Rapid, unified incident response and mitigation.

Resource Sharing: Shared expertise, intelligence, and security tools.

Proactive Defense: Threat hunting and preemptive security measures.

paloalto

Radically transform your SOC

AI-driven threat prevention & detection:

100% In SE Labs Ransomware Test

AI-driven investigation:

75% Less manual work

Agentic AI-driven response:

98% Reduction in MTTR

257%

ROI in the Forrester TEI

FORRESTER®

paloalto NETWORKS | CORTEX

As Leaders....

- Ask about your attack surface. Can't protect what you don't see.
- Get regular threat briefings from your security professionals.
- Look to reduce technical complexities and move to platformization.
- Value your most precious resource–people–by leveraging technology.
- Be ready. Have an incident response plan and retainer. Can't do it alone.
- Join forces. Scale resources and make it a team sport.
- Know your "technical debt". This is the real denominator.

Let’s keep simple:
How to know if you’re doing okay.

What’s your **Mean Time to Detect?**

What’s your **Mean Time to Respond?**

Thank You

paloaltonetworks.com

About Unisys

My name is Justin Davis, Director of Integration and Innovation for Unisys Cybersecurity Solutions Delivery. Thank you to the Chairs of the Communications and Technology and Local Government Committees for inviting Unisys to present this important issue today. Our team provides a range of cybersecurity solutions to clients globally, which includes partnerships with over 240 public sector entities. Unisys is proud to be a partner with the Commonwealth, not only because Blue Bell, Pennsylvania is home to our headquarters, but for decades we have seen successful partnerships across the state. With over 150 years of serving the government, our company has strong foundations in innovating technology, with examples dating back to 1945, when we partnered with the University of Pennsylvania to deliver the first programmable, general-purpose electronic digital computer. This not only demonstrated the value of our institutional partnerships, but we also answered our nation's call to provide innovative technology to support national security. Our continued partnership with the Commonwealth underpins the importance of cooperation between private and public entities to face the evolving cybersecurity threat landscape with solutions that effectively protect critical data and systems for your constituents.

My testimony today will not only examine potential threats to state and local government technology infrastructure, but it will also include a discussion about the effects your constituents are likely facing as a result of data breaches outside of your network responsibilities. Cybercrime and fraud are systemic problems nationwide, and this committee has opportunities to explore that will empower your constituents to protect themselves.

Cybersecurity Risks for Government Systems

The threat landscape for state and local governments continues to evolve, driven by the persistent use of ransomware and the growing adoption of artificial intelligence (AI) by threat actors. Compared to 2023, there was a 51% decrease in state and local government reporting of ransomware attacks in 2024 (Sophos, 2024). However, the severity of ransomware attacks increased significantly, with 98% of incidents resulting in data encryption (Sophos, 2024). Organizational recovery costs more than doubled in 2024, from ~$1.21 million to $2.83 million (Sophos, 2024). Seventy-two percent of ransom demands exceeded $1 million, and 37 percent exceeded $5 million (Sophos, 2024). Fifty-four percent of victims paid the ransom, including some who had previously improved their backup strategies (Sophos, 2024).

In 2025, Emsisoft (2024) reported a mid-year trend indicating a 65 percent increase in ransomware attacks on government entities worldwide. In August 2025, the Pennsylvania Office of Attorney General was hit by a ransomware attack that disrupted internal systems and court cases (Office of Attorney General, 2025). The security incident also involved the potential breach of personal information, including names and social security numbers (Office of the Attorney General, 2025).

As we continue to see the implications of ransomware to state and local governments, we should also carefully monitor the evolving use of artificial intelligence. In November 2025, Anthropic published a report that implicated a Chinese state-sponsored group (GTG-1002) in using an artificial intelligence model to automate 80-90 percent of its espionage campaign against over 30 organizations, including government agencies (Anthropic, 2025). While this nation-state level threat has not been corroborated publicly by government officials yet, it represents a potential risk materializing for threats using artificial intelligence to improve their overall effectiveness. Industry reporting also indicates threat actors appear to be prototyping AI-driven ransomware, which may increase the effectiveness or frequency of successful attacks (ESET, 2025). These advances in adversarial use of artificial intelligence should be monitored closely and considered when evaluating modern security operations solutions.

Cybercrime Risks for Constituents

Constituents of the Commonwealth, like many across the world, have a high likelihood of being victims of data breaches. When we talk about victims, we often focus on the organizations that are targets of threats to steal private information. However, one could argue that the most vulnerable people are those whose information was compromised in a data breach.

The Identity Theft Resource Center (2025) reported that, globally, over 1.3 billion data breach notices were issued in 2024 to individual victims. This represented an approximately 211 percent increase compared to 2023 (Identity Theft Resource Center, 2025). While direct correlations between data breaches and cybercrime or fraud victimization are rare, data breaches arguably increase the vulnerability of victims to subsequent cybercrime and fraud.

Identitytheft.org (2025) indicated that one in three U.S. adults has experienced identity theft or fraud at some point, but many people may not report that they were victims. The median cost of fraud across all reported victims was approximately $500, with an average of approximately $4,800 (Federal Trade Commission, 2025).

The Federal Trade Commission (2024) reported that the median loss for government impersonation scams reached as high as $14,740 in 2024 (Federal Trade Commission, 2024). Some of the most vulnerable people are senior citizens who experience higher impacts than other age groups. For example, government impersonation victims over the age of 60 lost over $46,000 on average in 2024, which is about 199% higher than other age groups (FBI IC3, 2025). Victims over the age of 60 who lived in Pennsylvania lost $28,824 on average (FBI IC3, Pennsylvania, 2025).

The bottom line is constituents of the Commonwealth are at risk for cybercrime and fraud, regardless of where the cybercriminals obtain the information needed to target their victims.

Cybersecurity & Fraud Recommendations for Constituents

Organizations routinely invest in cybersecurity awareness programs to educate employees on recognizing threats and adopting safe practices. These programs often combine clear messaging with actionable steps, such as enabling multi-factor authentication and monitoring for suspicious activity. State and local governments throughout the Commonwealth can apply a similar model to their

constituents, focusing on practical measures that reduce personal risk. A campaign that emphasizes locking credit reports by default, monitoring financial accounts, and using multi-factor authentication would mirror proven strategies in the private sector while addressing the unique vulnerabilities of individuals in the state (FBI, 2023).

The FBI often publishes guidance that good cyber hygiene begins with recognizing threats such as phishing, social engineering, and credential theft, and pairing awareness with actionable defenses like multi-factor authentication (MFA) and strong password practices (FBI, 2023). These measures are foundational to preventing unauthorized access and reducing fraud exposure.

Freezing credit records with Equifax, Transunion, and Experian is an essential step to reducing the impacts of Identity Theft. Threat actors often exploit stolen personal data to open fraudulent accounts, and credit freezes significantly limit this risk. Similarly, encouraging constituents to monitor their bank accounts and financial statements regularly is essential to detecting fraud early.

Academic institutions across Pennsylvania could play a pivotal role by inspiring students to engage in community outreach. Federal programs such as the Cybersecurity Education and Training Assistance Program (CETAP), managed by the Department of Homeland Security, demonstrate how partnerships with schools can extend cybersecurity awareness beyond classrooms and into communities (Department of Homeland Security, 2024). Similarly, initiatives like NIST's Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) program show how collaboration among academia, government, and industry can create pathways for students to support local outreach efforts (National Institute of Standards and Technology, 2024). These models not only prepare the next generation of cyber professionals but also amplify awareness campaigns for vulnerable populations, including seniors and rural communities.

Benchmarking State and Local Government Success

The Commonwealth has an opportunity to consider some of the progress other State, Local, Tribal, and Territorial (SLTT) governments have made in collaborative cybersecurity. For example, SLTT governments in Maryland, Minnesota, New York, Ohio, and Oregon have made progress in strengthening cyber resilience through collaborative programs, which combine state leadership and funding with localized execution (Center for Internet Security, 2025). A few examples of SLTT success include prioritizing resource sharing, technical assistance, and training to address gaps that smaller jurisdictions face in the

absence of dedicated cybersecurity teams. Federal and state grant funding accelerated SLTT programs to deploy advanced endpoint protection, multi-factor authentication, and security awareness training (Center for Internet Security, 2025).

The State of Arizona also established a statewide Cyber Readiness Program, which provided SLTT governments with access to critical cybersecurity tools, including anti-phishing training, endpoint protection, and web application firewalls at no cost to participating organizations (Arizona Department of Homeland Security, 2025.). Arizona demonstrated how targeted investments can close security gaps and improve statewide resilience (Arizona Department of Homeland Security, 2025.).

For the Commonwealth, examining these successes offers a practical benchmark for designing a similar initiative that fosters public-private collaboration, maximizes grant funding, and delivers scalable solutions to protect critical systems and constituent data.

Securing the Commonwealth's Networks

Establishing Statewide Security Baselines

Pennsylvania has taken meaningful steps toward improving cybersecurity with pending bills, such as H. 1219, which establishes the Office of Information Technology and sets statewide security standards, and S. 373, which enhances governance and oversight. Other measures, such as H.R. 997 on protecting personal information and S. 415 addressing ransomware, demonstrate a growing commitment to privacy and deterrence. H. 705 focuses on grid resilience, and H. 1188 limits risks from foreign adversary-controlled applications. These are important moves, but they should be part of a broader strategy. The Commonwealth needs a comprehensive security baseline built on frameworks like NIST, CSF and CIS Controls, applied consistently across local governments and third-party providers. That baseline should include identity governance, multi-factor authentication, endpoint protection, secure configurations, and disaster recovery plans. Looking ahead, future legislation should go further by requiring continuous monitoring, immutable backups, and planning for post-quantum cryptography. Workforce development and automation also need attention to close talent gaps and strengthen operational resilience (National Conference of State Legislatures [NCSL], 2025).

Continuous Monitoring and Governance

The Commonwealth, in partnership with Unisys, has made significant progress in consolidating IT services through the Pennsylvania Compute Services (PACS) program, which has integrated several data centers into a single hybrid cloud environment. This initiative enhanced visibility and security across agencies, providing a foundation for modernization (Unisys, 2020). The next priority, however, is statewide continuous monitoring. Today, monitoring remains uneven. Some local government agencies have strong Security Operations Center (SOC) capabilities, while others operate with limited resources. A unified approach that integrates Security Information and Event Management (SIEM), Managed Detection and Response (MDR), and exposure management would give the Commonwealth the ability to identify threats in real-time and respond quickly.

Recent election cycles have demonstrated the value of dedicated monitoring for critical systems; however, these successes were tied to specific events rather than a permanent model (Pennsylvania Department of State, 2025). Continuous monitoring should become the standard, allowing local governments to benefit from the same level of protection. As part of that strategy, the Commonwealth should consider sending telemetry to a centralized Managed Security Service Provider's (MSSP) managed detection and response (MDR) platform. Through a centralized approach, MSSPs can deliver security orchestration, automation, and response (SOAR) with emerging innovations like agentic AI, which improve triage and analytics by leveraging insights across multiple clients (Radiant Security, 2025; Microsoft, 2025; Bussie, 2025). This approach would not only strengthen detection and response but also position Pennsylvania to take advantage of next-generation security operations.

Immutable Backups and Disaster Recovery Playbooks

Prevention is important, but it must be supported by a plan for rapid recovery. The Commonwealth should require immutable backups, isolated cyber vaults, automated runbooks and regular testing, such as quarterly restore exercises and tabletop drills across state and local government organizations. These measures are essential to maintain services such as water, healthcare, public safety, and revenue streams in the event of ransomware or supply chain attacks (MS-ISAC, 2025; NCSL, 2025). State and local entities consistently rank incident response and recovery as their top priority for both short-term and long-term planning,

which reflects the growing trend of attackers targeting backups and identity systems (MS-ISAC, 2025). Leveraging Federal Cybersecurity and Infrastructure Security Agency (CISA) resources and Multi-State Information Sharing and Analysis Center (MS-ISAC) shared services to standardize recovery metrics such as Recovery Point Objective (RPO), Recovery Time Objective (RTO), vault integrity, and privileged recovery procedures will shorten restoration times, reduce public impact, and protect taxpayer dollars (CISA, 2025; MS-ISAC, 2025).

Fostering Public-Private Partnerships

The Commonwealth should strengthen public and private partnerships to close capability gaps, reduce costs, and accelerate innovation. Collaboration across the state, which brings together agencies, counties, municipalities, school districts, and critical infrastructure operators, can deliver economies of scale for threat detection, vulnerability management, and incident response when paired with MS-ISAC services and vendor platforms (MS-ISAC, 2025; Route Fifty, 2025). CISA's updated SLTT support model, which includes direct access to grants, no-cost services, and regional advisors, along with the State and Local Cybersecurity Grant Program, creates opportunities to fund shared SOC, MDR, and endpoint protections, especially for smaller and rural jurisdictions (CISA, 2025). The Commonwealth should formalize a partnership framework that aligns procurement, performance reporting, and intelligence sharing to reduce tool fragmentation and provide a consolidated, risk-prioritized view of the state's security posture (CISA, 2025; NCSL, 2025).

Cyber Workforce Development and Automation Tool Investments

Persistent talent shortages necessitate a strategy that integrates workforce development with automation. The Commonwealth should invest in statewide programs, such as apprenticeships, cyber ranges, and internships, in collaboration with community colleges and universities. It should also establish cyber navigator teams to support counties and school districts, and deploy automation tools that enhance analyst productivity, including SOAR, validated playbooks, and AI-assisted triage (MS-ISAC, 2025; NCSL, 2025). Stable multi-year funding is critical because one-time grants do not provide the continuity needed for hiring and retention. Partnerships with CISA and MS-ISAC can supply curriculum, exercises, and managed services to ease the burden on smaller jurisdictions (CISA, 2025; MS-ISAC, 2025). Aligning job classifications and compensation with market realities while embedding automation into detection and response workflows will improve containment times and strengthen the resilience of Commonwealth services (MS-ISAC, 2025; Route Fifty, 2025).

Advanced Security Measures

Continuous Threat Exposure Management (CTEM)

Cybersecurity cannot be treated as a one-time exercise. Threat actors exploit gaps that appear between scheduled assessments, and those gaps often remain unnoticed until an incident occurs. Continuous threat exposure management (CTEM) provides an ongoing view of vulnerabilities and misconfigurations across networks, applications, and identities. Instead of relying on annual or quarterly scans, CTEM enables state and local governments to identify and prioritize risks in near real time. This approach reduces the window of opportunity for attackers and ensures that remediation efforts focus on the most critical exposures. For a state with diverse local government and third-party providers, CTEM offers a practical way to maintain a consistent security posture across the enterprise (CISA, 2025; Center for Threat-Informed Defense, 2025).

Post-Quantum Cryptography (PQC)

Quantum computing is not a distant concept. It is an emerging reality that will eventually render current encryption standards obsolete. The Commonwealth should begin planning for this transition now. Post-quantum cryptography (PQC) provides algorithms designed to withstand quantum attacks, and early adoption will prevent a scramble when quantum capabilities mature. A first step is conducting a cryptographic posture assessment to identify where legacy encryption is used and where future vulnerabilities may exist. From there, state and local government organizations can develop a roadmap for integrating PQC into critical systems. This is not only about protecting classified data. It is about ensuring that citizen records, financial systems, and essential services remain secure for decades to come (NIST, 2024; Cloud Security Alliance, 2025; IEEE Spectrum, 2025).

Agentic AI and Security Orchestration, Automation, and Response (SOAR)

The cybersecurity talent shortage is not going away, and manual processes cannot keep pace with the modern threats. Agentic AI and SOAR technologies offer a way forward by automating routine tasks and accelerating incident response. These tools can triage alerts, execute predefined playbooks, and adapt workflows based on context. This reduces the time it takes to contain and remediate threats. For Pennsylvania, this means faster detection, fewer false positives, and improved resilience without requiring a proportional increase in staffing. Automation does not replace human judgment. It amplifies the effectiveness of security teams and ensures that critical decisions are made with

speed and precision (ISACA, 2025; Belfer Center for Science and International Affairs, 2025; Coalition for Secure AI, 2025).

Conclusion

Unisys is proud to serve as a trusted partner to the Commonwealth in its mission to strengthen cybersecurity. Our work together has demonstrated what collaboration can achieve, from enhancing visibility across agencies to laying a foundation for resilience. The challenges ahead are significant, and they will continue to evolve. Local governments face the most significant resource challenges and can benefit from state-led initiatives. Ransomware, identity theft, and emerging technologies like quantum computing and AI-driven attacks require a unified approach and a commitment to continuous improvement. By advancing statewide security baselines, investing in monitoring and recovery, and preparing for future risks, Pennsylvania can lead the way in protecting critical systems and safeguarding its citizens. Unisys is ready to collaborate with the Commonwealth to assess and remediate issues faced by local governments. We appreciate the opportunity to support this mission and remain committed to working alongside the Commonwealth to ensure its networks and services are secure today and ready for tomorrow.

Meet the Unisys Team

Dr. Justin Davis

Director,
Cybersecurity Integration & Innovation

Edward Tillman

Director,
Client Security Executive

Phil Swarbrick

Vice President,
Cybersecurity Services

Kannan Arunachalam

Regional Director,
COPA Client Management

References

AARP / Javelin Strategy & Research. (2025, March 25). Identity fraud and scams cost Americans $47 billion in 2024. Retrieved from: https://www.aarp.org/money/scams-fraud/javelin-identity-theft-report-2024/

Arizona Department of Homeland Security. (n.d.). Statewide Cyber Readiness Program. Retrieved from https://azdohs.gov/statewide-cyber-readiness-program

Belfer Center for Science and International Affairs. (2025). The rise of agentic AI: Infrastructure, autonomy, and America's cyber future. Retrieved from https://www.belfercenter.org

Bussie, B. (2025, June 25). From playbooks to partnerships: How agentic AI redefines the MSSP model. MSSP Alert. Retrieved from https://www.msspalert.com/perspective/from-playbooks-to-partnerships-how-agentic-ai-redefines-the-mssp-model

Center for Internet Security (MS-ISAC). (2025, August 11). Strengthening critical infrastructure: SLTT progress & priorities. Retrieved from https://www.cisecurity.org/insights/white-papers/strengthening-critical-infrastructure-sltt-progress-priorities

Center for Internet Security. (2025). Strengthening critical infrastructure: SLTT progress & priorities (Vol. 2). Retrieved from https://learn.cisecurity.org/strengthening-critical-infrastructure-sltt-progress-priorities-full-report-vol2

Center for Threat-Informed Defense. (2025). INFORM: Best practices assessment tool. Retrieved from https://ctid.mitre.org/inform

CISA. (2024). Partnerships and collaboration. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/topics/partnerships-and-collaboration

CISA. (2025). Continuous diagnostics and mitigation program. Retrieved from https://www.cisa.gov/resources/programs/continuous-diagnostic-mitigation

Cloud Security Alliance. (2025). A practitioner's guide to post-quantum cryptography. Retrieved from https://cloudsecurityalliance.org

Coalition for Secure AI. (2025). CoSAI principles for secure-by-design agentic systems. Retrieved from https://www.coalitionforsecureai.org

Cybersecurity and Infrastructure Security Agency (CISA). (2025). Cybersecurity resources for state, local, tribal, and territorial partners. Retrieved from https://www.cisa.gov/resources-tools/resources/sltt

Cybersecurity and Infrastructure Security Agency (CISA). (2025). State, local, tribal & territorial cyber information sharing program. Retrieved from https://www.cisa.gov/resources-tools/programs/state-local-tribal-territorial-cyber-information-sharing-program

Emsisoft. (2024, January 9). The state of ransomware in the U.S.: Report and statistics 2024. Emsisoft Blog. https://www.emsisoft.com/en/blog/46288/the-state-of-ransomware-in-the-u-s-report-and-statistics-2024/

Emsisoft. (2025, September 17). Summer 2025 by the numbers: Ransomware statistics. Emsisoft Blog. https://www.emsisoft.com/en/blog/46903/summer-2025-by-the-numbers-ransomware-statistics/

ESET. (2025, August 27). ESET discovers PromptLock, the first AI-powered ransomware. ESET. https://www.eset.com/us/about/newsroom/research/eset-discovers-promptlock-the-first-ai-powered-ransomware/

FBI. (2023). FBI highlights online safety tips during Cybersecurity Awareness Month. Federal Bureau of Investigation. https://www.fbi.gov/contact-us/field-offices/norfolk/news/fbi-highlights-online-safety-tips-during-cybersecurity-awareness-month

Federal Bureau of Investigation. (2024). 2024 Elder Fraud State Report – Pennsylvania. Internet Crime Complaint Center (IC3). Retrieved from https://www.ic3.gov/AnnualReport/Reports/2024EFState/#?s=42

Federal Bureau of Investigation. (2024). 2024 Internet Crime Report. Internet Crime Complaint Center (IC3). Retrieved from https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Federal Trade Commission. (2024, June 14). FTC data shows major increases in cash payments to government impersonation scammers. Retrieved from

https://www.ftc.gov/news-events/news/press-releases/2024/06/ftc-data-shows-major-increases-cash-payments-government-impersonation-scammer

Federal Trade Commission. (2024). Consumer Sentinel Network Data Book 2024. Federal Trade Commission. Retrieved from https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024

Federal Trade Commission. (2024, June 14). FTC data shows major increases in cash payments to government impersonation scammers. Federal Trade Commission. Retrieved from https://www.ftc.gov/news-events/news/press-releases/2024/06/ftc-data-shows-major-increases-cash-payments-government-impersonation-scammers

Federal Trade Commission. (2024). Consumer Sentinel Network Data Book: Median for government impostor scams (all payment types). Federal Trade Commission. Retrieved from https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf

Federal Trade Commission. (2024, June 14). *FTC data shows major increases in cash payments to government impersonation scammers*. Federal Trade Commission. Retrieved from https://www.ftc.gov/news-events/news/press-releases/2024/06/ftc-data-shows-major-increases-cash-payments-government-impersonation-scammers

Geller, E. (2025, May 21). AI drives cyber strategies, security execs say. Cybersecurity Dive. https://www.cybersecuritydive.com/news/ai-security-risks-executives-survey/748664/

IEEE Spectrum. (2025). The urgency of post-quantum cryptography adoption. Retrieved from https://spectrum.ieee.org

Identity Theft Resource Center. (2025, January 28). ITRC 2024 Annual Data Breach Report. Identity Theft Resource Center. Retrieved from https://www.idtheftcenter.org/publication/2024-data-breach-report/

Identity Theft Resource Center. (2025, July). ITRC H1 2025 Data Breach Analysis. Identity Theft Resource Center. Retrieved from https://www.idtheftcenter.org/wp-content/uploads/2025/07/ITRC-H1-2025-Data-Breach-Analysis.pdf

IdentityTheft.org. (2025). Identity theft facts and statistics. Retrieved November 19, 2025, from https://identitytheft.org/statistics/

ISACA. (2025). The rise of the agentic AI defender. Retrieved from https://www.isaca.org

Javelin Strategy & Research. (2024, April 10). 2024 Identity Fraud Study: Resolving the Shattered Identity Crisis. Retrieved from: https://www.javelinstrategy.com/research/2024-identity-fraud-study-resolving-shattered-identity-crisis

Mandiant. (2023). M-Trends 2023 special report. Mandiant. https://www.mandiant.com/resources/reports/m-trends-2023-special-report

Microsoft. (2025, April 1). Transforming public sector security operations in the AI era. Microsoft Security Blog. Retrieved from https://www.microsoft.com/en-us/security/blog/2025/04/01/transforming-public-sector-security-operations-in-the-ai-era/

National Conference of State Legislatures (NCSL). (2025, October 10). Cybersecurity 2025 legislation. Retrieved from https://www.ncsl.org/technology-and-communication/cybersecurity-2025-legislation

NIST. (2024). Post-quantum cryptography standards. Retrieved from https://www.nist.gov

NSA. (2024). National Centers of Academic Excellence in Cybersecurity. National Security Agency. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence

Pennsylvania Department of State. (2025, March 19). Election security in Pennsylvania. Retrieved from https://www.pa.gov/agencies/vote/elections/election-security

Pennsylvania Senate GOP. (2025, June 4). Senate approves Phillips-Hill's cybersecurity legislation. https://www.pasenategop.com/news/senate-approves-phillips-hills-cybersecurity-legislation

Pothen, J. (2024, June 20). FTC warns of cash losses to government impostors. Payments Dive. Retrieved from https://www.paymentsdive.com/news/ftc-federal-trade-commission-scam-fraud-cash-payment/719371/

Radiant Security. (2025, November 3). What happens to MSSPs and MDRs in the age of the AI-SOC?. Retrieved from https://radiantsecurity.ai/blog/mssps-and-mdrs-al-soc/

Route Fifty. (2025, July 31). State and local governments need a unified approach to cybersecurity. Retrieved from https://www.route-fifty.com/cybersecurity/2025/07/state-and-local-governments-need-unified-approach-cybersecurity/407053/

Sophos. (2024, August 14). The state of ransomware in state and local government 2024. Sophos News. https://news.sophos.com/en-us/2024/08/14/the-state-of-ransomware-in-state-and-local-government-2024/

Unisys. (2020, March 16). Commonwealth of Pennsylvania extends work with Unisys for secure hybrid cloud computing. Retrieved from https://www.unisys.com/news-release/copa-extends-work-with-unisys-secure-hybrid-cloud-computing/

Wood, C. (2025, August 11). Pennsylvania AG's systems down after 'cyber incident'. StateScoop. https://statescoop.com/pennsylvania-ag-dave-sunday-cyber-incident/

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.

The Authorities
PENNSYLVANIA MUNICIPAL AUTHORITIES ASSOCIATION

Joint Informational Meeting
House Communications and Technology Committee
House Local Government Committee
Informational Meeting on *Cybersecurity and Local Governments*

February 25, 2026

Testimony of:
Craig Fahnestock, Deputy Executive Director of Member Services

Good afternoon, Majority Chairmen Ciresi and Freeman, Minority Chairmen Ortitay and Miller, as well as members of the House Communications and Technology Committee and the House Local Government Committee. Thank you for your invitation to provide testimony on *Cybersecurity and Local Governments*.

My name is Craig Fahnestock, and I am testifying on behalf of the Pennsylvania Municipal Authorities Association (PMAA), which represents nearly 700 municipal authorities across the Commonwealth. Authorities provide essential services, including drinking water treatment and distribution, wastewater collection and treatment, solid waste management, and other community projects to roughly six million people in Pennsylvania. In addition, PMAA has over 500 associate members, including accountants, engineers, solicitors, and professional services consultants who provide expert support to our member authorities.

Background on Municipal Authorities

Under the Municipality Authorities Act (MAA), a municipal authority serves as an alternate vehicle for accomplishing public purposes that might otherwise be carried out directly by boroughs, cities, townships, or counties. Authorities finance their services primarily through user fees and often serve multiple municipalities, creating operational efficiencies and economies of scale that extend beyond political boundaries.

Regardless of size or geography, the mission of every municipal authority is the same: to deliver high-quality, reliable, and safe services at an affordable cost. Importantly, authority operations do not compete with other traditional components of local government budgets. For these reasons, the authority model is particularly well-suited to providing regional services.

Authorities may be created by a county, borough, city, or township, either individually or jointly. Once established, the authority manages all aspects of its operations, relieving the creating municipalities of complex and highly technical responsibilities. Authorities are governed by locally appointed boards, and meetings are conducted publicly in accordance with the Sunshine Act.

At the same time, the MAA prohibits authorities from duplicating or competing with existing enterprises serving substantially the same purposes. This structure ensures transparency, local governance, insulation from day-to-day political pressures, and a clear focus on serving the best interests of the communities involved.

In addition to the MAA, municipal authorities must comply with numerous state and federal laws, including environmental, public health, labor, procurement, ethics, and open records statutes. Authorities are required not only to meet current regulatory obligations but also to plan and budget for future requirements as they emerge. This extensive regulatory environment underscores the complexity of authority operations and highlights the importance of protecting the systems that support essential public services.

Cybersecurity and Critical Infrastructure

Municipal authorities share a fundamental responsibility: to provide uninterrupted essential services. Water, wastewater, and related systems are designated as critical infrastructure. Disruptions caused by ransomware, network intrusions, or operational technology breaches can pose serious risks to public health, environmental compliance, and public trust.

Authorities manage sensitive information, including customer data, employee records, financial information, and highly technical systems operations data. Most authorities rely on automated supervisory control and data acquisition (SCADA) systems and other operational technologies to manage treatment and distribution systems.

A successful cyberattack can result in service disruptions, regulatory violations, environmental harm, and significant financial loss. As information technology (IT) systems increasingly converge with operational technology (OT) systems such as SCADA, the potential attack footprint expands, elevating overall risk.

Municipal authorities are not unlike any other businesses or governmental agencies subject to attack. Simply put, it is not a matter of if, but when an authority will face a cyber threat.

The Evolving Threat Landscape

Cyber threats have become more sophisticated and increasingly targeted toward water and wastewater systems nationwide. Ransomware attacks against public infrastructure continue to rise, and hackers actively probe systems that may lack robust cybersecurity protocols.

Emerging risks now include the use of artificial intelligence (AI) tools to generate highly convincing phishing emails and impersonation attempts that are far more difficult to detect. Supply chain vulnerabilities also present growing concerns, as trusted vendors and third-party service providers can inadvertently introduce risk into otherwise secure environments. In addition, hostile actors have demonstrated increased interest in targeting critical infrastructure systems.

In light of these evolving and complex threats, municipal authorities must now plan not only for prevention, but also for detection, response, recovery, and long-term operational resilience.

PMAA's Role in Education and Preparedness

PMAA recognizes that municipal authorities operate essential public infrastructure. As stewards of these vital systems, authorities must be prepared to defend against increasingly sophisticated cyber threats that could disrupt operations, compromise sensitive data, or undermine public trust. To that end, PMAA works continuously to educate and support its members in strengthening cybersecurity awareness, preparedness, and response capabilities. Our approach is comprehensive and ongoing, recognizing that cybersecurity is not a one-time initiative but an evolving responsibility.

PMAA provides education and training to members through multiple channels to ensure consistent access to timely information and practical guidance. These efforts include:

- **Written communications**, including cybersecurity-focused articles in our bimonthly magazine *The Authority* (October 2025 issue – Cybersecurity Month), which highlight emerging risks, practical mitigation strategies, and case studies relevant to municipal authorities.
- **Electronic communications**, sharing alerts, threat advisories, and guidance issued by federal partners such as the Environmental Protection Agency (EPA), the Cybersecurity and Infrastructure Security Agency (CISA), and other relevant agencies. These communications help ensure members receive up-to-date information about evolving vulnerabilities and recommended protective measures.
- **Interactive education and engagement**, including webinars, podcasts, workshops, symposiums, an online member community, and annual conference programming dedicated specifically to cybersecurity awareness, governance responsibilities, regulatory developments, and implementation of best practices.
- **Access to associate members and subject-matter experts**, including professionals specializing in cybersecurity consulting, risk assessments, incident response planning, and cyber insurance coverage. This network provides authorities with practical resources and technical expertise tailored to the unique operational and budgetary realities of our members.

Recognizing that cybersecurity readiness requires both policy support and financial investment, PMAA has further demonstrated its commitment by adopting the following resolution as part of our 2026 advocacy platform:

> ***Resolution 9-26***
> *RESOLVED, That PMAA support legislation providing assistance and funding to municipal authorities for the implementation of new and necessary technologies, as well as employee training, to meet ongoing cybersecurity threats.*

Beyond technology controls such as firewalls and encryption, one of the most important elements of cybersecurity is the human factor. Even the most advanced systems can be compromised through human error, social engineering, or insufficient awareness. Municipal authority employees, board members, contractors, vendors, and even customers can serve as a critical first line of defense when properly informed and trained. Accordingly, PMAA regularly emphasizes the following core practices to foster organizational resilience:

1. **Cybersecurity Awareness.** Learn to recognize potential threats such as suspicious emails, text messages, unexpected password reset requests, unfamiliar attachments, and unusual system behavior.

2. **Building a Security Culture.** Cybersecurity is not solely an IT department function. It is an organizational responsibility that extends from executive leadership and board members to frontline staff.
3. **Phishing Prevention and Email Hygiene.** While hardware and software safeguards are necessary, the human element remains a primary vulnerability. A significant percentage of breaches begin with a single click. Ongoing simulated phishing exercises and training are essential.
4. **Network Segmentation and Internet of Things Security.** Today, everything is connected. Secure practices include isolating operational systems from administrative networks and maintaining segmentation between employees, customers, and guest networks to minimize the impact of a potential breach.
5. **AI for Good and Bad.** While emerging technologies such as AI can improve system monitoring and threat detection, these same technologies also enable more sophisticated scams, impersonation attempts, and automated attacks.

Operational Example: Workforce and Training Investments

Many municipal authorities recognize that technology alone cannot defend against cyber threats. As a result, they treat cybersecurity as an operational priority that is embedded into daily practice, employee expectations, and organizational culture.

Many authorities have implemented structured security awareness programs that require all employees, from executive leadership to frontline operators, to complete regular cybersecurity training. These programs typically include mandatory onboarding instruction, refresher courses, and monthly simulated phishing exercises designed to replicate real-world attack scenarios.

When employees click on simulated malicious links, they are immediately directed to targeted retraining modules that reinforce proper response protocols. In some cases, repeated failures may result in temporary suspension of email privileges or additional supervisory review. This structured approach creates accountability while reinforcing a culture of vigilance.

By investing in workforce education, municipal authorities strengthen what is often the most vulnerable point in any cybersecurity framework: the human element. Continuous training, testing, and reinforcement help transform employees from potential entry points for attackers into active participants in system protection and resilience.

Key Challenges Facing Municipal Authorities

- **Funding Constraints.** Cybersecurity upgrades such as multi-factor identification, endpoint detection and response, network monitoring, system redundancy, and incident response planning require ongoing investment. Not all municipal authorities have the staffing capacity or budget flexibility to implement these upgrades. Smaller authorities often lack dedicated cybersecurity staff and rely on contracted IT providers. Moreover, cybersecurity is not a one-time expense; it requires sustained investment in software subscriptions, hardware upgrades, audits, insurance, and training. While the federal State and

Local Government Cybersecurity Grant Program has provided limited funding, municipal authorities in Pennsylvania are not currently eligible for this funding, and the program is scheduled to sunset in 2026.

- **Workforce and Expertise Gaps.** Experts, industry data, and workforce studies show there is a national shortage of cybersecurity professionals. Municipal authorities, particularly in rural areas, cannot compete with private-sector salaries. Shared service models, regional assistance, and state-level technical support could help bridge this gap.
- **Regulatory and Compliance Uncertainty.** As mentioned earlier, authorities must comply with extensive environmental and public health regulations while navigating evolving cybersecurity expectations. Clear, coordinated guidance and technical assistance are critical to avoid unfunded mandates.
- **Operational Technology Security.** Many water and wastewater systems operate legacy control systems not originally designed with modern cybersecurity safeguards. Retrofitting and securing these systems can be technically complex and costly.

Legislative and Policy Recommendations

PMAA respectfully offers the following recommendations:

- **Clear Eligibility for Cybersecurity Grant Funding.** Municipal authorities should be clearly eligible for state-administered federal cybersecurity grants and future funding programs.
- **Creation of a Dedicated Funding Stream.** Establish a recurring state budget line item to support municipal authority cybersecurity infrastructure.
- **Statewide Cybersecurity Taskforce or Technical Assistance Program.** Create a centralized state resource to assist municipal authorities with risk assessments, incident response planning, threat intelligence sharing, and coordinated response during cyber events.
- **Enhanced Information Sharing and Incident Coordination.** Strengthen partnerships between state agencies, emergency management officials, and municipal authorities to ensure rapid notification and response to emerging threats.

Conclusion

Cybersecurity risk management is an ongoing and dynamic process of identifying, analyzing, evaluating, and addressing threats. Every municipal authority differs in size, operational complexity, and financial capacity. Therefore, flexibility is essential. Authorities must be empowered, not overburdened, with the tools, funding, and technical support necessary to protect critical infrastructure.

Investing in cybersecurity today is far less costly than responding to a successful attack tomorrow. Protecting Pennsylvania's water systems and other essential services is not merely an operational responsibility; it is a foundational obligation tied directly to safeguarding public health, preserving environmental quality, maintaining economic stability, and ensuring the long-term resilience of our communities. When these systems are secure and reliable, they protect families, support local businesses, sustain ecosystems, and reinforce public confidence in government's ability to deliver critical services without interruption.

Again, thank you for the opportunity to testify before you today. I am happy to answer any questions.

TESTIMONY BY
THE PENNSYLVANIA STATE ASSOCIATION OF
TOWNSHIP SUPERVISORS

BEFORE THE
HOUSE COMMUNICATIONS & TECHNOLOGY
AND LOCAL GOVERNMENT COMMITTEES

ON

LOCAL GOVERNMENTS AND CYBERSECURITY

PRESENTED BY

HOLLY FISHEL
POLICY AND RESEARCH DIRECTOR

FEBRUARY 25, 2026
HARRISBURG, PA

4855 Woodland Drive Enola, PA 17025-1291 www.psats.org
Telephone: (717) 763-0930 Fax: (717) 763-9732

Chairman Ciresi, Chairman Freeman, and members of the House Communications and Technology and Local Government Committees:

Thank you for inviting PSATS to present remarks on behalf of the 1,453 townships of the second class represented by our association. My name is Holly Fishel and I am the Policy and Research Director for PSATS.

PSATS is the Pennsylvania State Association of Township Supervisors and we are a nonprofit, nonpartisan organization committed to preserving and strengthening township government and securing greater visibility and involvement for townships in the state and federal political arenas. Our members cover 95% of Pennsylvania's land mass and represent 5.7 million Pennsylvanians — more residents than any other type of municipality in the commonwealth.

Technology is constantly evolving and cyber criminals are continually becoming more sophisticated. Municipalities across the Commonwealth need training, funding, and expertise to help mitigate these threats.

It is important to remember that not all municipalities are the same. Our largest member township has a population of more than 60,000 and our smallest has less than 100 residents. Some townships have dozens of employees; others may only have one or two part-time employees. Some may have an Information Technology department while others have a single computer. But all townships have sensitive data and provide vital services to their communities. These realities make a one-size-fits-all approach to cybersecurity impossible.

Education is key to preventing successful attacks. Being able to recognize suspicious emails, websites, and even phone calls are essential. Bad actors regularly impersonate the federal government and claim they will assist with renewing a township's SAM.gov registration for hundreds of dollars, when direct renewal is free and simple. Others impersonate vendors, utilities, banks, literally anyone with which a township does business. These attacks continue to grow in sophistication and artificial intelligence is accelerating the number and types of attacks.

Unfortunately, one click is all it takes. Phishing, where a deceptive email or website is used to impersonate a legitimate business or person and trick recipients into entering sensitive data like account numbers and passwords, accounts for 80 to 95 percent of all attacks. Townships are at risk for these attacks just like any other entity, because email is a normal part of everyday township operations.

Townships face escalating cybersecurity threats disguised as open records requests. Townships receive many open record requests delivered by highly suspicious email that the township must evaluate and answer. We see requests from out-of-state companies looking to use public township records for data harvesting on residents, businesses, and the vendors who do business with the township, often leveraging AI tools. Currently, the Right-to-Know Law fails to protect critical township records, including credit card numbers, bank account numbers, passwords, and usernames, putting taxpayer funds at risk. We contend that the RTKL should be amended to protect taxpayer funds, reduce the risk of identity theft for public employees and

officials, and eliminate the requirement to respond to emails that look like a phishing attack just because they contain an RTKL request.

Township officials receive email from residents, vendors, state and federal agencies, partners like PSATS, and countless others. We've seen cyber criminals impersonate vendors or change payment information on real invoices and become referred consultants from subscription accounting software. As criminals use advances in artificial intelligence (AI) to make their messaging appear legitimate, removing grammar errors, and mimicking the content of other emails a township receives, local officials need more education and tools to keep up.

Phishing provides an opening for criminals to follow up with other attacks, including malware like computer viruses, remote access to a victim's device, and spyware that gathers usernames, passwords, and financial information. Ransomware encrypts the victim's data and holds it hostage for ransom, or locks the device, making it impossible for the victim to even power it on.

Identifying vulnerabilities and evaluating potential impacts can help stop an attack before it starts. Implementing network security measures like firewalls, multi-factor authentication and regular software updates are important. Even the basics of creating difficult to guess passwords and regularly updating them are important actions to keep cyberinfrastructure safe. Regular data backups and off-site storage can help mitigate the impact of an attack.

Despite the rising importance of cybersecurity, the resources available to local governments are dwindling. According to a 2025 study by the Multi-State Information Sharing and Analysis Center (MSISAC), 68 percent of state, local, tribal, and territorial governments "lack direct funding to implement major cybersecurity priorities."

The Joint State Government Commission's January 2026 report, "Artificial Intelligence: Advisory Committee Recommendations on the Adoption and Use of AI in Pennsylvania" noted that the Commonwealth could lead the nation in cybersecurity by creating and implementing programs catered to local governments. The report cites recommendations to create and publicize cybersecurity bundles to local governments. Such a bundle could include referrals to Commonwealth-approved third-party cybersecurity vendors, IT professionals, and cyber insurance companies.

We encourage the commonwealth to develop materials and training programs to help educate local government officials on the ever-changing threats and best practices. The Joint State Government Commission report also suggested that the Commonwealth could create a .gov website where government officials could shop for cybersecurity bundles and review verified relevant cybersecurity information for immediate implementation. We encourage the legislature to look at new grants or revenue streams to provide risk assessments, secure local infrastructure, and protect data.

PSATS has served on the State & Local Cybersecurity Grant Program Committee whose goal is to help address local governments cybersecurity risks and threats using federal funding. This program secured funds for asset intelligence, intrusion detection services, and software

services to address cybersecurity risks and strengthen critical infrastructure. With limited federal funding and a finite menu of options, the committee prioritized county participation in the competitive grant program, followed by school districts and other municipalities. Given that municipalities are diverse in terms of their cybersecurity needs and capabilities, townships could benefit from options other than competitive grants, such as the bundling options mentioned.

Thank you for the opportunity to testify before you today.

TESTIMONY OF THE

PENNSYLVANIA SCHOOL BOARDS ASSOCIATION

BEFORE THE HOUSE COMMUNICATIONS AND TECHNOLOGY COMMITTEE

& HOUSE LOCAL GOVERNMENT COMMITEE

FEBRUARY 25, 2026

KEVIN BUSHER

PSBA CHIEF ADVOCACY OFFICER

Chairman Ciresi, Chairman Ortitay, and Chairman Freeman and Miller, and members of the Communications and Technology Committee and Local Government Committee, thank you for inviting the Pennsylvania School Boards Association (PSBA) to testify today on behalf of the 5,000 local public school leaders we represent. My name is Kevin Busher and I am not only the Chief Advocacy Officer for PSBA, but also a former nine-year veteran of the Lower Dauphin School Board in Dauphin County.

Public schools are entrusted with the safety, privacy and well-being of the students, families, and staff in their communities. In 2026, that responsibility extends far beyond the physical walls of school buildings. Today, it includes protecting the sensitive data and digital systems that underpin nearly every aspect of teaching, learning, transportation, communications, and school operations.

School districts, career and technical centers, and intermediate units —large and small— have become prime targets for cyberattacks. Our members face escalating incidents of:

- Ransomware attacks that lock down student information systems, payroll systems, and instructional platforms;
- Data breaches exposing sensitive student and staff information;
- Email phishing leading to financial fraud or compromised credentials; and
- Disruption of instructional time, sometimes for days, when core systems are shut down.

Most public school entities do not have dedicated cybersecurity departments or the financial means to support large-scale protections, yet they hold some of the most sensitive data of any public institution. When a breach occurs, it is not just an inconvenience — it is a direct threat to the safety and privacy of our children and employees.

To help frame the digital data discussion, consider that a student's 12 year academic career generates a digital footprint that begins in kindergarten and follows through to commencement, and beyond. You've probably heard the term "Big Data". Pennsylvania's schools have it sitting in server rooms, classrooms, and online educational systems.

The data includes personal details and contacts, assessments, assignments, grades, homework, health information, attendance history, transportation details, discipline records, special education records, communications, PSSA, PVAAS, PIMS records, and more. It's a staggering amount of private data for schools to manage, maintain, and protect. And the volume of data grows every day.

Here's one example to illustrate the enormity of the data archive. Every school year, Pennsylvania public school districts are required to report more than 40 data sets to the Pennsylvania Department of Education's PIMS system. These data sets contain dozens of data points per student. For an average district, this process amounts to millions of private data records stored in both our local student information systems and the PDE PIMS data warehouse.

Between July 2023 and December 2024, 82% of K-12 schools experienced a cyber incident, according to a survey by the nonprofit Center for Internet Security.[1] A single cyber incident can shut down school operations entirely for days after the incident is detected.

Further, cyberattacks can lead to:

- An inability to deliver instruction due to disabled learning platforms;
- Closure of school buildings because attendance and communication systems are offline;
- Delayed payroll for educators and staff;
- Loss of access to critical special education or medical documentation;
- Weeks or months of recovery and forensic investigation; and
- Costly remediation that diverts resources from classrooms.

Cybersecurity is a school safety issue. We are appreciative of the change made in last year's School Code bill that allows schools to use School Safety and Security grant funding for cybersecurity. Most public schools simply lack the budget required for modern cyber defenses, cybersecurity personnel, or system-wide upgrades. Many districts operate with aging infrastructure that cannot support current security expectations.

Because public school entities do not have the financial means to employ cybersecurity professionals, they are forced to rely heavily on IT generalists who are stretched thin and often responsible for both instructional technology and network operations. However, our schools are constantly fighting a 10,000 pound, multi-headed, data security monster. Unlike our staff, that monster never sleeps. It kicks at network doors and rattles digital locks 24 hours a day, 7 days a week. There are no days off, holidays or summer vacation.

Public schools also rely on hundreds, if not thousands of software applications and vendors, each with different security practices. Without consistent standards or oversight, our systems are only as secure as the weakest third party platform.

---

[1] https://www.k12dive.com/news/k-12-schools-experienced-cyber-incident-cis/741915/

While our members are committed to doing everything within their power to protect themselves from cyberattacks, the reality is that they cannot meet the scale of this challenge alone. We respectfully urge the committee and General Assembly to consider:

- Providing school entities with dedicated, sustained cybersecurity funding. Stable, recurring funding is essential to building and maintaining adequate cyber defenses rather than one-time grants.
- Providing school entities with support for modernizing network infrastructure, implementing security best practices, enhancing data backups and recovery capabilities, conducting security assessments and penetration testing, and hiring or contracting with cybersecurity professionals.
- The state currently provides school entities with guidance, resources and best practices with regards to physical school safety and security. Yet the state has not included a digital safety, privacy, and protection strategy for all students, teachers, and parents. We would encourage policymakers to consider creating a statewide agency or office which could provide schools with guidance and resources related to digital safety, privacy, and protection.
- Establishing clear cybersecurity standards for K–12 vendors would help protect student data and reduce districts' risk exposure.
- Establishing a standardized, nonpunitive reporting structure would help schools quickly access help during a cyber incident and allow agencies to identify statewide patterns or vulnerabilities.

Cybersecurity is now one of the most pressing issues facing public education. When a school district is attacked, the victims are not institutions — they are students, teachers, families, and communities. Our members are committed to protecting our students both in our classrooms and online. But we cannot meet this challenge without strategic partnership and support. Thank you for your attention to this critical issue and for your commitment to the safety and stability of our public schools. I am happy to answer any questions.