TESTIMONY BY
THE PENNSYLVANIA STATE ASSOCIATION OF
TOWNSHIP SUPERVISORS

BEFORE THE
SENATE LOCAL GOVERNMENT AND COMMUNICATOINS AND
TECHNOLOGY COMMITTEES

ON

CYBER SECURITY

PRESENTED BY

BRIAN RENGERT
DEPUTY DIRECTOR OF GOVERNMENT RELATIONS

JANUARY 31, 2024
HARRISBURG, PA

Good afternoon, Chairwoman Brown, Chairwoman Pennycuick, Chairman Kearney and Chairman Dillon and members of the Senate Local Government and Communications and Technology Committees. My name is Brian Rengert and I am the Deputy Director of Government Relations at the Pennsylvania State Association of Township Supervisors (PSATS).

Thank you for allowing me the opportunity to present remarks on behalf of the 1,454 townships of the second class represented by our association. PSATS is 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. Townships of the second class cover 95% of Pennsylvania's land mass and represent more residents — 5.7 million Pennsylvanians — than any other type of municipality in the commonwealth.

First, let me start off by saying I am not a cyber security expert. However, I think we can all agree that as technology has become integrated into every part of our life, the threat from cyber criminals has never been more real. Whether it's the Fortune 500 company or the individual consumer, we are all vulnerable and local government entities are not immune from the threat.

More legislation or mandates will not solve the problem. Technology is constantly changing, and cyber criminals are becoming more sophisticated every day. Laws and mandates will not be able to keep up. More training and funding, along with the proper expertise to help mitigate these threats, is what is needed.

When crafting a plan, it is important to remember that not all municipalities are the same. Our largest member township has a population of 62,707 and our smallest a population of less than 20. Some townships have dozens of employees; others may only have one part-time employee. Some have their own police departments, others do not. Some may have an IT (Information Technology) department while others have a single computer. But all have sensitive data, and all provide vital services to their communities.

These realities make a one-size-fits-all approach to cyber security impossible.

State and local governments should be planning for a cyber-attack like they plan for a natural disaster. It is not a matter of if it happens, but when it happens. That is why PSATS rolled out the PSATS Cyber Advantage Program in 2023 to first and foremost protect from an attack and second deal with the consequence of an attack.

The program begins with a free assessment of the municipality's needs and includes options for: cyber insurance that protects a township from exposures; cyber liability insurance that protects a township if a third party is damaged due to negligence; data breach insurance protecting the township from some costs associated with a data breach including restoring a system, forensic investigation, notifying impacted individuals as well as free credit monitoring; and finally cyber extortion insurance protecting from ransomware.

Education is key to preventing an attack. One click is all it takes. How many of us have received a questionable email or text message and had to think twice about it before acting? Or failed to think twice before clicking? It is estimated that 88% of all breaches have a human element. And

the threat is always changing. In addition to the traditional phishing email, we've seen cyber criminals impersonate real vendors or change payment information on real invoices.

PSATS also launched cyber education as well as a monthly newsletter with the latest tips, news and updates to help townships prepare for these challenges. In 2023, we offered multiple webinars on the topic as well as three in person courses at our State Conference and regional forums. In 2024 we will be offering a course entitle "A Hacker's Perspective: Why Your Network is my Playground." Ransomware and phishing attacks continue to be leading cyber threats to local government and private citizens alike.

The advances in artificial intelligence (AI) will cut both ways ...some to help bad actors and some to help prevent bad actors, so the early and thoughtful appropriate regulation is critical. Either way, AI will increase the risk of cyber threats. For example, generative AI will be able to remove the spelling and grammar errors that often mark spam messages. The good news is that it is not expected that AI will not be developed enough to be able to create its own ransomware attackers in the next 2 years but will be working towards it.

We would encourage the state to develop materials and training programs to help educate local government on the ever-changing threats, best practices for protecting themselves, and how to respond to a threat. It is also important that municipalities and local officials have a response plan if they are attacked.

Unfortunately, protecting from cyber-attacks also requires resources. We would encourage the legislature to look at new grants or revenue streams to provide risk assessments, securing of local infrastructure, and protection of data.

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 also important. Regular data backups and off-site storage can help mitigate the impact of an attack. Finally, continuous education for our local government users is essential.

We appreciate you bringing attention to this issue and look forward to working with you to find a solution.