



FOR IMMEDIATE RELEASE

Oct. 5, 2017

Wolf Administration Highlights Cybersecurity Initiatives to Protect Pennsylvanians

Harrisburg, PA – In the wake of high-profile cyber attacks targeting businesses, governments and other organizations, the Wolf administration is reminding Pennsylvanians to take appropriate steps to protect their personal and financial data.

“We depend on technology and the Internet in so many ways, which is why all of us must do our part to keep them secure,” said Governor Wolf. “No one is immune to cyber attacks. However, there are many simple things we can do that reduce the chances of being a victim.”

Leaders of several state agencies also spoke today about their efforts to protect the public from cyber threats.

“The frequency and complexity of cyber attacks, especially following the Equifax data breach, reinforce the need for everyone and every organization to have conversations about cybersecurity and to make plans to protect themselves,” said Secretary of Banking and Securities Robin L. Wiessmann. “In response to this challenge, today we have launched a cybersecurity guide for consumers, produced by a collaboration of 10 state agencies and offices. The online guide will help consumers protect themselves and their families as they navigate the internet in their daily lives.”

The guide includes tips to prevent identity theft, protect passwords, keep children safe online and secure mobile devices.

View the online cybersecurity guide at <https://www.pa.gov/guides/cybersecurity/>.

The Office of Administration (OA) oversees cybersecurity for agencies under the Governor's jurisdiction and is a leader among states in security. Pennsylvania recently earned top honors for cybersecurity from the National Association of State Chief Information Officers (NASCIO) for cloud security using risk-based multifactor authentication.

Currently in use for cloud email and storage, the service reduces the risk of unauthorized access by requiring users to provide information, in addition to a user name and password, to verify their identities. OA intends to implement the safeguard on additional systems in the future.

“Pennsylvania has a multi-layered cybersecurity program to protect its systems and the data within them,” said Erik Avakian, Chief Information Security Officer for the commonwealth. “We work to continuously improve our protections to respond to new and emerging risks.”

Watch this video about PA’s award-winning initiative at: <https://youtu.be/iMyaJr7aI50>.

The Department of State (DOS) takes full advantage of OA’s expertise as part of its strategy to safeguard the commonwealth’s electoral system, including the statewide voter registration database.

“We know there are those who would attempt to disrupt elections through cyber intrusions,” Secretary of State Pedro A. Cortés said. “We constantly monitor for threats and vulnerabilities, and will continue our vigilance and our collaborations with law enforcement and security agencies. As the cornerstone of democracy, our election infrastructure must be a priority for increased protection.”

State agencies are also focused on planning and preparedness. In 2016, Pennsylvania was one of the first states in the nation to hold an exercise focused on the response to a prolonged, widespread power outage, such as from a cyber attack. In August, the Public Utility Commission, Governor’s Office of Homeland Security and Pennsylvania Emergency Management Agency took part in a first-ever transnational exercise to test responses to a large-scale power outage event.

“An orchestrated cyberattack on our utility infrastructure could have the same wide-reaching and long-lasting impact on our communities as hurricanes or other natural disasters – not only disrupting the flow of electricity, but also disrupting many other vital systems and services that we depend upon,” said Public Utility Commission (PUC) Chairman Gladys M. Brown. “These are called ‘Black Sky’ events, and the citizens of Pennsylvania should know there is a massive amount of work taking place, mostly behind the scenes, involving our utilities; state agencies; emergency responders and other organizations to better prepare for cyber and physical attacks, strengthen critical systems, share information about current and future threats, and ensure that essential services are as resilient as possible.”

Additionally, the Pennsylvania Emergency Management Agency recently updated the State Emergency Operations Plan, which includes adoption of the Pennsylvania Cyber Incident Annex (PICA), to better prepare for – and respond to – and recover from potential cyberattacks. The PICA brings together several state agencies, unified by the common goals of threat response, asset response, and intelligence coordination and support. The PICA also supports the Pennsylvania Criminal Intelligence Center (PaCIC), which is managed by the Pennsylvania State Police and is the state’s primary designated all hazard fusion center comprised of analyst and subject matter experts from local, state, and federal agencies.

MEDIA CONTACTS:

Dan Egan, Office of Administration, 717-772-4237
Ed Novak, Banking and Securities, 717-783-4721
Wanda Murren, State, 717-783-1621
Nils Hagen-Frederiksen, Public Utility Commission, 717-418-2701
Ryan Tarkowski, Governor’s Office of Homeland Security, 717-783-5556

###