pennsylvania
OFFICE OF ADMINISTRATION

Testimony

House Republican Policy Committee

March 28, 2022

Commonwealth Cybersecurity

Office of Administration

John MacMillan

Commonwealth Chief Information Officer

Chairman Causer and Members of the House Republican Caucus Policy Committee, I am John MacMillan, Deputy Secretary for Information Technology and Chief Information Officer (CIO) for the commonwealth.

I was appointed in March 2015 and possess over 35 years of experience in the Information Technology (IT) industry. For almost 19 years, I worked for one of the world's leading IT companies throughout several states with some notable accomplishments. In New York, New Jersey, and Washington, I guided customers through complex application development initiatives. In Texas and Georgia, I aided in efforts on a data center outsourcing project. In Pennsylvania and Ohio, I worked on projects related to data center consolidation, operations, and standardization, achieving operational effectiveness and saving clients millions of dollars.

Since 2010, our Enterprise Security Office has been led by Erik Avakian, making him the longest-tenured state Chief Information Security Officer (CISO) in the country. Under Erik's leadership, our cybersecurity program has grown and matured to become a model program to other states. Erik is highly sought out for his insights, experience, and thought leadership. Erik has attained a vast array of security experience and expertise including security delivery, strategy and design, architecture, risk assessment, policy, compliance, incident response, and investigations. Erik holds industry certifications including Certified Information Systems Security Professional (CISSP), Certified Risk and Information Systems Control (CRISC), Certified Information Security Manager (CISM), and Certified Information Security Auditor (CISA). He is an Executive Committee member for the Multi-State Information Sharing and Analysis Center (MS-ISAC) and collaborates with members of the National Association of State Chief Information Officers (NASCIO) and the Pennsylvania State Fusion Center (PACIC).

Cybersecurity is a paramount concern and a major priority for the Office of Administration (OA) in our role as an internal IT service provider. We are proud to be recognized as a leader among states for information technology and cybersecurity. Since 2015, OA has received 28 information technology and cybersecurity awards, which are listed in the Appendix.

Unfortunately, the reality for any private business or public entity is not *if* a cyber-attack will affect them, but *when*. Globally, organizations spent over $86 billion in 2017 to defend against cyber-attacks and that figure is estimated to rise to $170 billion in 2022. The potential costs of a successful attack can also be substantial. South Carolina had a data breach at its Department of Revenue that cost the state over $30 million. In the private sector, Equifax paid $650 million to settle claims stemming from a 2017 data breach, while Target incurred at least $158 million in costs for its massive breach several years ago. There are numerous additional examples.

Every other year, NASCIO conducts a survey to identify and prioritize the top policy and technology issues facing state government. Not surprisingly, cybersecurity and risk management have been the #1 priority every year since 2013. CIOs point to governance, budget and resource requirements, data protection, training and awareness, insider threats, and third-party risk among their top concerns in 2022. In addition to these concerns, we would also highlight the need for additional staff, which is hampered by a lack of qualified candidates, competition with the private sector for available talent, and obsolete or aging infrastructure that constrains staff and limits growth or transformation.

One of the most challenging elements of cybersecurity is the rapidly evolving threat landscape. The nature and sophistication of security risks are constantly shifting, requiring organizations to quickly adapt and respond each and every time. By way of example, organizations worldwide are continuing to respond to the recent discovery of an exploitable vulnerability found within a widely used piece of open-source code known as Log4j. Log4j can be found in the programming of many websites, applications, cloud computing services, and other technology products. Bad actors were actively using this vulnerability against organizations to gain unauthorized access to data, deploying malware, and creating new administrator accounts with elevated privileges.

Earlier this month, the cybersecurity firm, Mandiant, announced in a report that at least six states were compromised by state-sponsored hackers from China. The report cites the use of significant new capabilities, from new attack vectors to post-compromise tools and techniques. The report stated that within hours of the Log4j vulnerability announcement, this hacker group shifted its tactics to include this new exploit. Because these threat actors are always looking for and attempting to use possible vulnerabilities in software and systems, we have to always remain vigilant by keeping our threat monitoring capabilities updated, fortifying our systems and networks, keeping our staff informed and mobile so that they are able not only to react to threats, but to fend off such attacks. This necessary diligence requires significant resources.

Another example you may recall is the cyber-attack in 2020 against the cybersecurity technology company, SolarWinds. In this incident, hackers compromised the company’s security and inserted a vulnerability into its software, which was then unknowingly deployed to customers through software updates. These hackers used this vulnerability to move undetected through systems and networks. According to published reports, the attack ended up compromising hundreds of governmental organizations, including several federal agencies. Despite the commonwealth being a customer of SolarWinds, no evidence exists that any of our systems were compromised using this vulnerability. However, we had to quickly mobilize resources to react to that rapidly emerging and evolving security issue. These are just two examples of the challenges we constantly face, demonstrating how preventing and responding to cybersecurity threats is a marathon that never ends.

OA’s security services include safeguards such as firewalls, network intrusion prevention, spam blocking, advanced malware protection, and virus protection. The security statistics are telling:

- In a recent month, there were 27.8 billion attempts to attack our firewall.

- In 2021, there were 333 billion attempted hacks on commonwealth systems, inclusive of the enterprise firewall, intrusion prevention system, and Internet Proxy blocked events.

- Over the past 12 months, approximately 760 million incoming email messages arrived at our perimeter. Of those, 387 million, or 51 percent, were blocked as spam or malicious by our email filtering service. Without this service, each user on our email platform would receive an extra 14 messages containing spam or malicious emails every day.

Other key security services that OA provides include end-user security awareness training, risk management services, policy compliance assessments, code reviews, and vulnerability scans. For example, we perform vulnerability scans and code reviews of all new applications deployed in our data centers before they go live on the Internet. If security flaws are identified, application developers can fix the problems before they result in a security issue. Based on the number of attack attempts against our Internet-facing applications, this service has been instrumental in limiting the risk of inadvertent data exposure.

Training for employees and contractors who use IT resources is another pillar of our cybersecurity program. Most security incidents are the result of human error of some kind, such as clicking on a malicious link in an email. We require the annual completion of end-user security awareness and acceptable use training to ensure that our users understand how to recognize and report potential threats. There is also specialized security training for IT administrators and other users with elevated privileges. Training courses are reviewed and updated annually in conjunction with stakeholders such as agencies, the Office of General Counsel, and the Department of General Services. We also test the effectiveness of our training throughout the year with exercises meant to simulate real-world phishing attempts. When a user responds incorrectly to an exercise, we can provide immediate feedback about why they should have recognized the potential threat, what they should have done in response, and a recommendation for additional training. And when our users respond correctly and identify phishing threats, we recognize them positively for their efforts.

OA publishes IT policies to provide guidance to agencies and suppliers for securing IT resources. These policies can be found on the OA website, under Policies. Key policies related to information security include IT Policy SEC000 - Information Security Policy and Management Directive 205.34 Amended - Commonwealth of Pennsylvania Information Technology Acceptable Use Policy. Additionally, we have policies, standards and tools for email and data encryption, strong passwords, firewalls, incident reporting and response, physical security of IT resources, mobile device security, remote access and other topics.

In addition to the wide array of cyber defense and prevention measures I just described, we also have a detailed incident response procedure (IRP) that outlines the respective roles and responsibilities of each organization when responding to an

IT security incident. The IRP covers all phases of an incident and establishes the mobilization of the teams needed to effectively respond to the incident. When a potential security incident is identified, we conduct a thorough IT forensic analysis of system logs, security monitoring tools, and other sources.

OA collaborates on cybersecurity matters with the General Assembly through its IT leadership, with counties through our partnership with the County Commissioners Association of Pennsylvania (CCAP), in academia through our partnership with Harrisburg University, and our newly established partnerships with several cities and Intermediate Units. OA provides the General Assembly's IT leadership with enterprise cybersecurity advisories and awareness of existing cybersecurity solutions. OA has also engaged with the General Assembly's IT leadership through the Enterprise Technology Security Council (ETSC) Security Governance Workgroup. This group provides direction on strategy, investment, and policy matters to optimize spending, allocate resources appropriately, and minimize risk.

From an organizational perspective, a concentration of people in a centralized service model enhances our information security competencies. As part of the Shared Services initiative that started in July 2017, we continue our efforts to hire resources and offer training and career opportunities to support business process automation so agencies can serve the residents of Pennsylvania effectively and securely. Based on a national study published in October 2020, over 75% of states use a centralized service model, like OA, in this context.

OA's collaboration with local governments enables them to leverage our security awareness training and anti-phishing exercise capabilities while we help to absorb some of their costs for these services. We are also helping the counties increase their information security capabilities through the deployment of Center for Internet Security (CIS) network security monitoring and management services. This solution, referred to as Albert sensors, is already deployed in 46 counties. The estimated cost to deploy sensors in the remaining 21 counties is between $375,000 and $575,000.

Albert sensors provides network security alerts for both traditional and advanced network threats, helping organizations identify malicious activity. This cost-effective solution uses software combined with the expertise of the CIS 24x7 Security Operations Center (SOC) to provide enhanced monitoring capabilities and notifications of malicious activity. The staff in OA already receives alerts and notifications from the CIS SOC. This consistent approach benefits all Pennsylvania residents served by counties and the state.

Building on this collaborative approach, we would strongly recommend the creation of a Cybersecurity Coordination Board as contemplated in HB 1362. Such a board would be a new, effective, and cost-efficient way to enhance collaboration across the public and private sectors with respect to cybersecurity matters.

While we are proud of our robust cybersecurity program and confident in our ability to protect commonwealth systems and data, we can never rest on our laurels. The bad actors are constantly upping their game, and it is our challenge to stay one step ahead of their continuous escalation. We must accomplish this within the constraints of our available funding, staff and other resources. As mentioned earlier, the need to prioritize cybersecurity activities can require the reallocation of resources from other projects, thus delaying their progress and completion. We are excited about opportunities for cybersecurity funding in the American Rescue Plan Act (ARPA) of 2021 to support cybersecurity investments by both state and local governments and welcome the opportunity to explore additional funding to strengthen our security posture in the face of new and emerging threats. We encourage investing in preventative measures for the greater good.

On behalf of the Office of Administration staff, we appreciate the opportunity to submit testimony to this Committee.

*** END OF TESTIMONY ***

APPENDIX

The following table summarizes a list of national awards and recognition received since 2015.

Year	Organization	Description
2021	NASCIO	**Winner**, Emerging and Innovation Technologies, DHS Pandemic Electronic Benefit Transfer Robotic Process Automation
2021	NASCIO	Finalist, Digital Services: Government of Business, DOT Construction Documentation System
2021	NASCIO	Finalist, Data Management, Analytics and Visualization, Opioid Open Data Dashboard
2021	Center for Digital Government	Grade B+, Digital States Survey
2020	NASCIO	**Winner**, Data Management, Analytics and Visualization, DOT Maintenance IQ Data Visualization
2020	NASCIO	Finalist, Digital Services: Government to Citizen, REAL ID
2020	NASCIO	Finalist, Cybersecurity, Key Security Risk Indicators through Cyber Analytics and Correlation
2019	NASCIO	**Winner**, Enterprise IT Management Initiatives, IT and HR Shared Services
2019	NASCIO	Finalist, Digital Services: Government to Citizen, PA Child Enforcement System and Job Gateway Integration
2019	Center for Digital Government	**Winner**, Government Experience Award, Customer Service Transformation and Child Support/Job Gateway Integration
2019	Government Technology	Top 25 Doers, Dreamers and Drivers, Erik Avakian
2018	StateScoop	2018 Top 50 in State IT
2018	NASCA	**Winner**, Personnel, IT and HR Shared Services
2018	Center for Digital Government	Grade B+, Digital States Survey
2018	NASCIO	**Winner**, State CIO Special Recognition, Center of Excellence for Electronic Grants
2018	NASCIO	Finalist, Government to Business, Environmental ePermitting Platform
2018	Government Technology	Top 25 Doers, Dreamers and Drivers, John MacMillan

Year	Organization	Description
2018	Governor's Awards for Excellence	OA Open Data Team
2017	StateScoop	Top 17 State and Local Cybersecurity Leaders to Watch, Erik Avakian
2017	NASCIO	Thomas M. Jarrett Cybersecurity Scholarship Recipient, Erik Avakian
2017	NASCIO	**Winner**, Cybersecurity, Risk-Based Multi-Factor Authentication
2017	NASCIO	Finalist, Government to Business, eInspection Mobile Application
2017	NASCIO	Finalist, Government to Citizen, myCOMPASS Mobile App
2016	NASCIO	Finalist, Enterprise IT Initiatives, Department of Human Services Advanced Enterprise Web Services Security and Governance
2015	GovInfoSecurity	Top 10 Influencer in Government IT Security, Erik Avakian
2015	NASCIO	Finalist, Cybersecurity, Advanced Cyber Analytics
2015	NASCIO	Finalist, Improving State Operations, PennDOT Mobile Highway Construction App
2015	NASCIO	Finalist, Disaster Recovery/Security and Business Continuity Readiness, Security Breach Exercise