pennsylvania
OFFICE OF ADMINISTRATION

Testimony

Senate Communications and Technology Committee

Cloud Security for State, County, and Local Governments

March 13, 2023

Office of Administration

Christopher Dressler, Acting Chief Information Security Officer

Chairwoman Pennycuick, Chairman Dillon, members of the Senate Communications and Technology Committee, thank you for the opportunity to appear before you to testify about cloud security for state, county, and local governments.

My name is Christopher Dressler. I was appointed as Acting Chief Information Security Officer for the Commonwealth in 2022. I have 27 years of experience in information technology and cybersecurity. I started my public sector career at the Department of Revenue, where I held positions as an IT Manager and Information Security Officer. In 2018, I was promoted to be Information Security Officer for the Department of Revenue, Department of State, Department of Labor and Industry, Department of Banking and Securities, and Department of Insurance.

The Office of Administration (OA) is responsible for human resources, information technology, equal employment opportunity, continuity of government, and records management for state agencies under the Governor's jurisdiction. We also provide services and support to several independent boards and commissions.

Cybersecurity is a paramount concern and a major priority for OA. In a recent month, there were approximately 38 billion unauthorized attempts to connect to the Commonwealth's network. We blocked them each time, but it requires constant vigilance, software upgrades, and keeping pace with the latest hacking techniques to maintain the security of Commonwealth systems and data. Over the past 12 months, approximately 815 million incoming email messages arrived at our perimeter; of those, nearly half were blocked as spam or malicious by our email filtering service.

OA has a comprehensive cybersecurity program that includes multiple layers of monitoring and defenses to prevent unauthorized access, a robust framework of common industry practices, policies and procedures, and training and education for users. We constantly evaluate our cybersecurity practices and capabilities to safeguard against potential threats. Collaboration is a key component of our cybersecurity program. We work closely with our partners in federal, state, and local government, higher education, law enforcement, and the private sector to share information and resources related to cybersecurity.

OA's collaboration with the County Commissioners Association of Pennsylvania (CCAP) enables its members to leverage our security awareness training and anti-phishing exercise capabilities. Over 70,000 county employees are licensed to participate in these services. OA is also working with many counties to increase their information security capabilities through the deployment of Center for Internet Security (CIS) network security monitoring and management services, also known as Albert sensors. This turnkey solution provides a centrally managed service for monitoring and alerting of cyber threats. Notifications are sent in real-time through

an automated system that identifies traditional and advanced threats on a network, facilitating rapid identification of threats and attacks.

OA has also partnered with the City of Philadelphia on an agreement and cost model to expand security awareness training and phishing exercise services to nearly 25,000 city employees.

In the fall of 2022, the Federal Emergency Management Agency announced $185 million in funding, with up to $5.2 million for Pennsylvania, through the State and Local Government Cybersecurity Program (SLGCP). In accordance with the grant requirements, OA and PEMA have established a Cybersecurity Planning Committee to develop a comprehensive strategic plan and identify projects that will leverage SLGCP funds. The committee's membership includes the Governor's Office of Homeland Security, Pennsylvania State Police, Department of State, and other state agencies, as well as CCAP, Pennsylvania State Association of Township Supervisors, Pennsylvania State Association of Township Commissioners, Pennsylvania State Boroughs Association, Pennsylvania Association of Intermediate Units, Central Susquehanna Intermediate Unit, and the Pennsylvania Municipal League. Pennsylvania was among the first states to submit a plan to FEMA for approval. Funding in the first year will be used to continue and expand cybersecurity services available to local governments from the Office of Administration. These services are currently funded by an expiring election security grant. Local governments will be able to apply for competitive grants from the Commonwealth in the second through fourth years of the SLGCP.

These partnerships save real taxpayer dollars by leveraging economies of scale to lower licensing costs, reducing duplication of work across government entities, and expanding knowledge sharing and incremental improvement.

OA collaborates on cybersecurity matters with the General Assembly through its IT leadership. We provide the General Assembly's IT leadership with enterprise cybersecurity advisories and awareness of existing cybersecurity solutions. OA also engages with the General Assembly's IT leadership through the Enterprise Technology Security Council (ETSC) Security Governance Workgroup. We also partner with Harrisburg University on professional development and training for cybersecurity, as well as hosting an annual Cybersecurity Summit attended by hundreds of federal, state, and local governments, school districts, and universities.

Because of OA's leadership and collaboration, Pennsylvania is nationally recognized among states for information technology and cybersecurity. Since 2015, OA has received over 30 information technology and cybersecurity awards. Notably and most recently, the Center for Digital Government cited a focus on cybersecurity for

Pennsylvania's improvement to an A- grade in the 2022 Digital States Survey. Only six states earned a higher grade.

OA's commitment to cybersecurity extends to our utilization of IT services in the cloud. The cloud is fundamentally a data center managed by a third party in which the applications, computing, and/or storage takes place on the servers in the data center. By utilizing vetted and trusted cloud-based services, organizations, such as the Commonwealth do not have to manage physical servers, which reduces IT costs, improves operations, and can enhance security. OA utilizes a mix of traditional on-premises IT services that are hosted in Commonwealth-managed data centers, IT services that are hosted by a third party, and IT services that operate in a hybrid or multi-cloud model.

Commonwealth agencies can consume cloud-based infrastructure, software, and business process services when business requirements, financial resources, and policy compliance converge. For example, state agencies can utilize software as a service (SaaS). SaaS makes use of a cloud infrastructure to deliver one application to many users, regardless of their location, instead of the traditional model of one application per device. SaaS also gives agencies the ability to customize or configure applications for their specific environments. Besides SaaS, there are other cloud application programs that agencies can utilize to meet their needs.

OA has been utilizing cloud technology for almost a decade. In 2014, we entered into a contract for a hybrid cloud offering on-demand, scalable compute services to state agencies. A major benefit to this approach is that it allows agencies to purchase services when they need them to give greater flexibility and efficiency while saving money. For example, the Department of Revenue experiences a significant compute service need spike during tax season. The main purpose of this approach is to provide better service to our customers while reducing costs for technology infrastructure refreshment.

In 2017, OA formalized a Cloud Use Case Review Process to evaluate the potential use of cloud computing services. It includes reviews and approvals by a Cloud Services Review Committee comprised of subject matter experts in cybersecurity, networks, legal, procurement, and policy. The cybersecurity portion of the review includes identity and access management, application and data security, threat and vulnerability management, incident response, and monitoring and notification. The legal review ensures appropriate contract terms exist for security requirements. The policy review evaluates whether the use case meets all applicable IT policies, including policies for cybersecurity.

Following this comprehensive review, the cloud use case is reviewed by an Enterprise Architecture Review Committee with leadership from OA's Enterprise

Security Office, Enterprise Solutions Office, and Technology Service Office. This process has been updated and refined over the years as cloud computing has continued to evolve. Having a well-established and documented process helps to:

- Ensure that information technology services are aligned with business capabilities they underpin.
- Ensure architectural and solution building blocks are developed and reused, leading to consistent and repeatable practices in achieving enterprise-wide systems integration.
- Enable exploration of enterprise architecture feasibility initiatives as cost effective enterprise solutions.
- Increase transparency and awareness by incentivizing agencies to work together to share technology solutions.
- Create opportunities for cost savings through group contract agreements.

Cloud computing presents cybersecurity benefits for the Commonwealth. For example, cloud security provides centralized data protection controls, such as intrusion prevention, malware protection, identity and access controls, and encryption. Additional benefits include higher availability for applications and systems through service level and uptime commitments; improved regulatory compliance by leveraging solutions that meet government (federal and state) standards and guidelines; reduced costs through scalability, operational support, and infrastructure updates; and improved protection from common attacks such as DDoS (distributed denial of service).

Like other technology innovations, cloud computing also creates new challenges for cybersecurity that did not exist previously. Cloud implementations require organizations to enable appropriate cybersecurity controls and maintain a level of active management to help mitigate risks. Proper configuration of the cybersecurity controls in a cloud environment is essential to ensuring adequate protections of resources and data are in place. For example, data breaches remain a threat, and data breaches have been attributed to the cloud. A national accounting company recently suffered a ransomware attack that resulted in the theft of 6TB of corporate data. One of the exposed cloud servers contained unencrypted credentials to the accounting firm's customer accounts. Misconfigurations and inadequate change control within the cloud solution can make cloud resources vulnerable to attack, leading to reputational, customer, and financial damage. Application interfaces are the "front door" of the cloud and are used by customers to interact with the solution or service. These interactions occur over the Internet which is not secure. Therefore, it is imperative that secure connections are available and access controls are properly configured to interact with the cloud-based application or service. Finally, there is limited visibility into the cloud provider's environment. System and application logs "paint the picture" and provide insight into what is going on or what

has happened when a security issue or event occurs. However, organizations utilizing the cloud service are solely dependent on the cloud service provider for security issue remediation and incident response.

These challenges highlight the need to remain engaged with cloud providers and collaborate with them to ensure appropriate configurations are implemented. OA works to identify the necessary cybersecurity requirements for each cloud service utilized and enable access for the Commonwealth to maintain oversight and visibility into data in the cloud. The Cloud Use Case Review process is designed to assist in this review and encourage information sharing for informed discussions and decisions.

Millions of residents rely on technology, including cloud technology, to get the services they need from state agencies. OA is committed to enabling the business of state government and meeting citizen expectations for digital services while preventing and defending against cyberattacks and reducing vulnerability and risk of cyberattacks. We will continue to utilize industry best practices and rely upon national resources and frameworks to ensure our cyber health. Cloud computing has provided tremendous opportunities to innovate, operate more efficiently, engage with customers, and reduce costs for IT services. With the proper contractual terms and conditions and cybersecurity controls that address requirements, the cloud can be a great benefit to state and local governments and the Pennsylvanians we all serve.

Again, Chairwoman Pennycuick, Chairman Dillon, members of the Senate Communications and Technology Committee, thank you for the opportunity to appear before you to testify and provide information about cloud security for state, county, and local governments. I am happy to answer any questions that members may have on this matter.

Appendix A

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

Year	Organization	Description
2022	Center for Digital Government	Grade A-, Digital States Survey
2022	NASCIO	Finalist, Government to Citizen, DOR My PA Tax Hub
2022	NASCIO	Finalist, Information and Communications Technology, DHS Mass Text Messaging for Human Services Recipients
2022	NASPE	Winner, Eugene H. Rooney, Jr. Award for Innovative State Human Resource Management Program, Commonwealth Employee Resource Center
2022	Governor's Awards for Excellence	OA, DHS, PennDOT Find My Ride Apply
2021	NASCIO	Finalist, Emerging and Innovation Technologies, DHS Pandemic Electronic Benefit Transfer Robotic Process Automation
2021	NASCIO	Finalist, Digital Services: Government to 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
2021	Governor's Awards for Excellence	DOS Act 77 Implementation Team
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	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
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