pennsylvania
OFFICE OF ADMINISTRATION

Testimony

Senate Communications and Technology Committee

<u>Commonwealth Information Technology Services, Cybersecurity, and SB 810</u>

October 30, 2019

Office of Administration

John MacMillan

Commonwealth Chief Information Officer

Senator Phillips-Hill, Senator Santarsiero, and Members of the Committee, I am John MacMillan, Chief Information Officer (CIO) for the commonwealth.

On behalf of Governor Tom Wolf, Office of Administration (OA) Secretary Michael Newsome, and OA staff, thank you for the opportunity to appear before this Committee to discuss commonwealth information technology (IT), cybersecurity, and Senate Bill 810.

First, I'd like to share a little background about myself. I was appointed Deputy Secretary for Information Technology and CIO in March 2015. I have over 33 years of experience in the IT industry. For almost 19 years, I worked for one of the world's leading IT companies. I have had the opportunity to assist customers in several states, including New York, New Jersey and Washington, with application development initiatives in property management and social services. In Pennsylvania and Ohio, I was involved in projects related to data center consolidation, operations, and standardization that achieved operational effectiveness and saved millions. I also had the chance to work with customers in Texas and Georgia on data center outsourcing.

With me today is Erik Avakian, Chief Information Security Officer (CISO) for the commonwealth. Erik has served in this role since June 2010. He is responsible for the information security strategy, governance, technical standards, security policies, risk management, compliance, and cyber-incident response. Prior to his appointment, Erik served as Deputy CISO starting in 2007. Over the past 18 years, Erik has assembled a vast array of security experience and expertise including security delivery, strategy and design, architecture, risk assessment, policy, compliance, incident response and investigations. He has led numerous enterprise initiatives to further improve the commonwealth's security posture. Erik holds numerous industry certifications including Certified Information Systems Security Professional (CISSP), Certified in Risk and Information Systems Control (CRISC), Certified Information Security Manager (CISM), Certified Information Security Auditor (CISA), and is a Certified Government Chief Information Officer (CGCIO). He is an Executive Board member for the Multi-State Information Sharing and Analysis Center (MS-ISAC), a member of the National Association of State Chief Information Officers (NASCIO), and the Pennsylvania State Fusion Center (PACIC).

Nationally, Pennsylvania has become a recognized as a leader in information technology and cybersecurity. In the past several years, the commonwealth has received numerous national awards including:

Year	Organization	Description
2019	NASCIO	Winner, Enterprise IT Management Initiatives, IT and HR Shared Services
2019	NASCIO	Finalist, Government to Citizen, Child Support Enforcement System and JobGateway Integration Initiative
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
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
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

To understand information technology in the commonwealth today, it is helpful to have background on how we have evolved to our current state, as well as our need for continued flexibility to respond to changes in the IT marketplace.

The Office for Information Technology (OIT) within OA oversees enterprise technology for the commonwealth. When it was originally established in 1958, OA implemented the first centralized computer application (payroll) and provided IT guidance to agencies through its Bureau of Central Data Processing and the Bureau of Management Methods. Since its inception, OA has provided services to agencies under the Governor’s jurisdiction and to independent boards and commissions. Core services include, but are not limited to, setting policy and architecture standards, setting strategic direction and reviewing strategic plans, establishing IT governance, reviewing strategic projects over certain thresholds, inventorying applications for system upgrade planning, managing data standards and open data, as well as direct service provision for network, telecommunications, data center, email, disaster recovery and continuity planning, cybersecurity, enterprise resource planning (ERP), and other enterprise services.

Over the years, as technology has changed, so too have the services and organizational structure of OIT. Through the mid- to late nineties most agencies had their own IT departments to manage systems, such as applications, hardware, software, etc. This resulted in significant duplication of functions and resources. Beginning in the mid-nineties, OA began to consolidate the commonwealth’s technology infrastructure functions and services through the creation of a managed services relationship with an external supplier to maintain the mission-critical mainframe and server environments for multiple agencies. As client server technology became more prevalent, OA established the Enterprise Data Center with security controls, heating, cooling, and floor space for agency servers. Additionally, the commonwealth standardized on a single email platform, an enterprise resource planning (ERP) platform, and data network. While these early initiatives yielded significant savings and efficiencies, agency IT organizations continued to operate in silos, while following OA policies and standards.

In 2017, Governor Wolf announced the IT and HR shared services transformation. The goal of the initiative was to optimize costs and improve efficiencies by focusing on service delivery. It is worth noting that Pennsylvania is ahead of some states in many areas of IT, such as infrastructure consolidation. Nationwide, more states are moving towards a centralized IT shared service model.

The approach to IT shared services includes:

- Eliminating redundancies to drive cost optimization and efficiencies.
- Transforming how services are delivered to allow the agencies to focus resources and funds on citizen-facing activities.
- Improving the return on investment of taxpayer funds through a coordinated, standardized approach to service delivery for IT services.
- Reducing gaps in productivity and expertise found between small, medium, and large agencies.
- Improving relationships and communication with stakeholders.

The shared services model organizes IT by service delivery areas and functions, rather than by agency, to better leverage IT assets across the enterprise. Today, agency-specific and line of business services are provided by six cross-agency delivery centers. These delivery centers are organized by IT service area and support multiple agencies with similar missions and functions, where possible.

The six cross-agency IT delivery centers are:

General Government (OA, Office of the Budget, Office of General Counsel, Governor's Office, Lieutenant Governor's Office, Education, General Services, Office of Inspector General, and Independent Boards and Commissions that are serviced by OA).

Public Safety (Corrections, JNET, Probation & Parole, State Police).

Employment, Banking & Revenue (Labor & Industry, Revenue, State, Banking & Securities, Insurance).

Health & Human Services (Human Services, Health, Drug & Alcohol Programs, Aging, Military & Veterans Affairs).

Conservation & Environment (Conservation & Natural Resources, Environmental Protection, Agriculture, Milk Marketing Board, Environmental Hearing Board).

Infrastructure & Economic Development (Community & Economic Development, Transportation, Emergency Management).

IT staff in the delivery centers focus on applications to support agency programs and business functions while the enterprise supports the technology policies, infrastructure, and services needed to run these applications. Enterprise functions include:

Technology Business Office Strategy and Management - establishes common approaches for IT service management, IT project management, IT training, IT policy & compliance.

Enterprise Solutions - builds, configures and maintains enterprise solutions, through a shared services model – enabling IT staff within the delivery centers to leverage solutions to further agency business missions.

Service Desk - establishes a more coordinated approach to managing incidents in the commonwealth.

Technology and Operations - provides enterprise network, telecommunication and data center services.

Cybersecurity - protects the commonwealth's network, data and applications from threats and attacks.

Since cybersecurity matters have been, and will continue to be, a major area of concern at the state and national level, I want to give further information and details to the Committee. Cybersecurity and protecting our citizens' data and privacy is of paramount concern and the top priority for OA. That said, the reality for any private business or public entity is not "if" a cyber-attack will affect them, but "when." The potential costs of a successful attack can be substantial. South Carolina had a data breach at its Department of Revenue that cost over $30 million. According to published reports, recent ransomware attacks in Atlanta and Baltimore cost those cities $17 million and $18 million, respectively, as well as taking many city services offline for weeks. Meanwhile, the costs of ransomware attacks against Luzerne County government and the Philadelphia Court System have yet to be disclosed. In the private sector, Equifax has 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.

One of the most challenging elements of cybersecurity is the quickly and constantly evolving nature of security risks. Because of those elements, global cybersecurity spending was over $86 billion in 2017 and will rise to an estimated $170 billion by 2022. Keeping up with, and trying to stay ahead of, cybersecurity threats and risks is a marathon that never ends.

One of the major benefits of the shared services transformation is the consolidation of cybersecurity functions for agencies under the Governor's jurisdiction. Centralizing cybersecurity functions is critically important because it enables more efficient identification and resolution of cyber incidents, while allowing IT staff to marshal resources necessary to quickly diagnose and mitigate a potential security incident. The response to a security incident requires coordination among multiple IT disciplines, systems, and vendors. Having a single chain-of-command structure removes barriers to needed information.

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

- In a recent month, there were 21.7 billion attempts to attack our firewall. We were able to repel them, but it requires constant vigilance, software upgrades, and keeping pace with the latest hacking techniques to maintain the security of commonwealth systems and data.

- The number of attempted hacks on commonwealth systems
  - per day: 703 million
  - per week: 4.9 billion
  - per month: 21.1 billion
  - per year: 253 billion

Over the past 12 months, of all incoming 1.5 billion email messages. Of those, 603 million email messages (40.2%) were blocked as spam or malicious by our email filtering service. Without the service, each of the 85,000 end users on our email platform would receive an extra 21 spam messages every day.

Other key security services that OA provides to all agencies include end-user security awareness training, risk management services, policy compliance assessments, code reviews, and 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 issues before they result in a security issue. Based on the number of attack attempts against our Internet-facing applications, the service has been instrumental in limiting the risk of inadvertent data exposure.

During the fall of 2018, OA further formalized the commonwealth's response to potential security incidents by creating a detailed incident response procedure (IRP). The document outlines the respective roles and responsibilities of each organization in response to an IT security incident. The IRP covers all phases of an incident from discovery to triage to investigation to remediation and establishes the mobilization of the business, IT, communications, and legal teams needed to effectively respond to the incident. Other states and local governments have expressed interest in emulating our procedure.

The IRP provides a repeatable process for addressing an IT security incident. When a potential security incident is identified, we conduct a thorough IT forensic analysis of system logs, security monitoring tools, and other sources to determine whether any data was exposed. If the incident is considered a data breach under the Pennsylvania Breach of Personal Information Act, Health Insurance Portability and Accountability Act (HIPAA), or any other applicable law, we follow all requirements related to providing notification to affected individuals and, in some cases, notice to the public, as well. Conversely, if a security incident does not meet the legal criteria for a data breach, there is no requirement to notify individuals or the public.

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

Turning back again to shared services, over the past 33 months, the new delivery model has reduced the need for over $123 million in additional funding ("cost avoidance") to the commonwealth through the:

- Consolidation of HR and IT personnel into OA to create a single service organization to support state agencies.
- Implementation of a collaborative governance structure to make shared decisions about investments and priorities.

- Establishment of a new financial model to fully and accurately identify and recover costs associated with IT and HR services.
- Creation of a matrixed reporting structure for technology operations and cybersecurity.
- Issuance of an annual customer satisfaction survey to track performance in areas including collaboration, value, partnership, meeting needs, and communication.
- Development of metrics to track performance and demonstrate the value of HR and IT services to support agency missions.
- Continued convergence of technology infrastructure, platforms, and applications to increase efficiency and reduce risk.
- Continued standardization of processes and sharing of resources across delivery center agencies.

On June 30, 2019, the consolidation and standardization phases of the shared services transformation were completed. We are now concentrating on continuous improvement of the delivery model, processes and procedures, as well as additional cost streamlining through collaborative decision-making in established governance processes and groups.

Optimization is an ongoing process that consists of technology, application portfolio, and training convergence for improved service delivery. With a portfolio of over 2,000 applications, varying processes, and multiple tools and contracts to optimize, the full benefits of the model will continue to be realized over the course of many years. Aligning our services to industry standards and the work completed to date has put us on the right path to implement those changes.

With shared services, all the delivery centers have significant success stories. Some examples of success stories are:

Conservation and Environment Delivery Center

- Agencies are sharing hardware and software (firewalls, core switches and SQL clusters) to optimize the costs of each agency buying and maintaining their own.
- Department of Environmental Protection (DEP) and Department of Conservation and Natural Resources (DCNR) will share specialized GIS equipment, such as printers and plotters, reducing future replacement costs, in addition to sharing GIS applications created within the individual agencies.
- One agency’s training system was expanded to serve 38 other agencies, allowing them to eliminate inefficient processes without having to build or buy their own modern system.

Infrastructure and Economic Development Delivery Center

- Three agencies now supported by one IT help desk instead of three.
- The Pennsylvania Emergency Management Agency (PEMA) is working to share data from 9-1-1 centers with the Department of Transportation to improve response to traffic incidents.
- All three agencies in the delivery center share cybersecurity expertise with each other.

Public Safety Delivery Center

- Department of Corrections (DOC) and PSP IT staff are working together on mobile device support, including enrollment, purchasing, planning, configuration, and deployment. They are also sharing details on operational support and processes for desktop services, resulting in the sharing of scripts and deployment information for a system upgrade, which improves their security posture. They are also sharing processes and queries for System Center Configuration Manager (SCCM).

Employment, Banking & Revenue

- Infrastructure services were consolidated across 5 agencies realizing $3M in cost optimization through elimination, reduction, or avoidance.
- Transitioned five agencies to a single, standardized framework for Application Management, Requirements Management and Test Management, which established a shared service model and reduced the need for dedicated resources for each agency.
- License sharing across agency devices reduced the commonwealth’s legal risk and expenditures by $200,000.

General Government

- OA is successfully able to transition Act 71 of 2018 and assume the State Civil Service Commission hiring activities into OA-HR. This includes transitioning 75+ staff as well as all infrastructure, applications and software supporting the civil service hiring processes. During the transition, excess infrastructure and software licensing was decommissioned by taking advantage of OA-IT enterprise services, creating a more cost-effective operation.
- Utility Bill Management solution allows the commonwealth to measure current energy usage against benchmarked years and can

determine if there are savings opportunities available through making building improvements or other energy savings projects. The commonwealth has also identified about 200 utility accounts which were previously unmanaged and are now able to include these in centralized strategic procurements to negotiate better pricing for these utilities. Individual agencies are using this data to better manage their own utilities and facilities.

- The Office of General Counsel, General Government IT, and Public Safety IT worked together to migrate the legacy DOC litigation tracking system data and merge with the current Matter Management System to create one true system of record. Additionally, the Matter Management System was updated to include specific fields and requirements to support DOC's processes and eliminated the need for duplicate data entry of case information into redundant systems resulting in operational efficiency gains.

Health & Human Services

- Multiple toolsets being used to monitor databases at the Department of Health (DOH) and the Department of Human Services (DHS) were consolidated onto a single platform for DHS to monitor database environments across the delivery center.
- Equipment was migrated to a single data center improving the supportability and resources.

While consolidation of IT through shared services has many benefits, we believe it is still appropriate for some programs and functions to remain in state agencies rather than OA.

The 9-1-1 program under the jurisdiction of Pennsylvania Emergency Management Agency is an example where the agency has the subject matter expertise required to effectively run the program, including its technology components.

Similarly, the Pennsylvania State Police has subject matter expertise with respect to public safety communications and the Statewide Radio Network (STARNet).

Even when a technology program is under the purview of an agency, OA remains available to collaborate and support. We co-chair the Public Safety Communications Council with PSP and are supportive of the mobile radio modernization work that will protect the existing investments in STARNet and improve communication.

It is also worth noting that the radio network must be under the jurisdiction of a public safety agency to license public safety pooled frequencies. Transferring PA STARNet to OA would make Pennsylvania ineligible under FCC guidelines to access and leverage these frequencies, including frequencies donated by the Justice Department and First Energy.

IT procurement is another function that more appropriately resides outside of OA. The Department of General Services (DGS) is the agency most knowledgeable about the Procurement Code. Having procurement in DGS also provides for important separations of duties. OA is the customer looking to purchase goods and services and DGS manages the process leading to the selection of a supplier and ongoing relationship management, rather than OA doing both.

In its current form, Senate Bill 810 takes a “one-size-fits-all” approach by consolidating IT procurement and agency programs like the ones I just mentioned when they are better situated outside of OA.

With respect to IT procurement, the companion bill to SB 810, HB 56, is even more problematic. The House bill currently contains language being promoted by a technology company that would create a larger market for its products. Specifically, software that captures screenshots and keystrokes on the systems on which it is installed. While the intent is purportedly to improve accountability for IT contractors working for state governments, it creates significant cybersecurity, privacy, and federal regulatory compliance concerns. The contractor monitoring legislation is soundly opposed by CIOs across the nation and has been defeated in multiple states. Further, the National Association of State Chief Information Officers (NASCIO), which has consistently remained neutral on proposed legislation, took the unprecedented step of issuing a statement in opposition:

“While NASCIO certainly supports contractor productivity, cost efficiency and successful project outcomes, legislation of this nature could introduce unnecessary risks to citizen data by essentially transferring ownership of private citizen data to a third party. This type of legislation also has the potential for unintended consequences, such as impacting a state’s cybersecurity insurance policy coverage. State CIOs inherently understand and appreciate the seriousness of protecting citizens’ data, and therefore do not support legislation that could serve to increase or introduce additional risk.”

IT, as you are aware, is a rapidly changing environment. The organization that supports it must be flexible as IT changes while driving cost optimization. The ability to respond quickly and leverage industry best practices requires OA to continuously evaluate its people, processes and technology to determine how we can best serve the commonwealth.

With shared services, we must continue to transition to the future in a way that does not impede service delivery, but does accommodate marketplace dynamics with speed. With any major initiative, adjustments may be required at any point in time. We need the flexibility to modify our services and our service delivery model in response to changes in the IT industry and the evolving expectations of state agencies and the Pennsylvanians we all serve. Like other steps of our journey, it is a multi-year, multi-phase initiative.

The key is flexibility. We need the ability to modify our services and our service delivery model as the IT industry changes. The current IT executive order is written to be broad and non-prescriptive for this reason. It gives OA the authority needed to manage the IT commonwealth enterprise and be flexible enough to address the rapid, unpredictable changes that happen in the IT world. Our concern is that SB 810 is prescriptive and would undermine our ability to be nimble enough to effectively manage the commonwealth IT enterprise and cybersecurity.

Therefore, when considering the possibility of legislation that affects IT, we would encourage the legislature to keep this needed flexibility in mind and to avoid legislation that is overly restrictive, requires updates on a regular basis, or has the potential for unintended consequences.

Finally, with IT, there always a question about the fiscal cost. There is good news. As a result of shared services and changes that we have made, we continue to optimize operating costs to make the best use of available funding. As Secretary Newsome made clear during OA's budget hearing in February 2019, we are all citizens and taxpayers who want our tax dollars to be used effectively and efficiently. We are bringing proven business practices, based on industry standards, to run an agency as complex as OA. Most importantly, we will continue to focus on our duty to taxpayers to ensure all IT expenditures are optimized so maximum value is provided to our customers at the lowest possible cost in collaboration with the lines of business we serve.

On behalf of Governor Wolf, Secretary Newsome, and the OA staff, we thank all of you who continue to support our work. Once again, thank you for your time and the opportunity to appear before this Committee.

*** END OF TESTIMONY ***