pennsylvania
OFFICE OF ADMINISTRATION

# Testimony

# House Appropriations Committee

# Commonwealth Information Technology

# February 26, 2019

Office of Administration

Michael Newsome, Secretary

Chairman Saylor, Chairman Bradford, and members of the Committee, I am Michael Newsome, Secretary of the Governor's Office of Administration (OA). On behalf of Governor Tom Wolf, thank you for the opportunity to appear before this Committee to discuss information technology (IT) in the commonwealth.

With me today is John MacMillan. He was appointed Deputy Secretary for Information Technology and Chief Information Officer (CIO) in March 2015. He comes to the commonwealth with over 32 years of IT industry experience. He spent almost 19 years with one of the world's leading IT companies and managed a diverse portfolio of public sector work. Previously, John assisted New York and Washington States with application development initiatives. With Pennsylvania and Ohio, he led projects related to data center consolidation, operations, and standardization that increased operational effectiveness and saved millions of dollars for taxpayers. He also had the chance to work with Texas and Georgia on data center outsourcing.

I am also joined by Erik Avakian, Chief Information Security Officer. The Chief Information Officers (CIOs) of our Delivery Centers (DC) are also present.

I would like to begin by telling you a little bit about my background. I started in my current role at the Office of Administration on January 5th of this year. Previously, I served on the Pennsylvania Liquor Control Board, to which I was nominated in December 2015 and confirmed unanimously by the Senate in April 2016.

My nearly four-decade career with private sector businesses included experience in accounting, finance, human resources, strategic planning, and management.

I worked with The Wolf Organization for 11 years, six of those years directly with our now Governor Tom Wolf, as Executive Vice President and Chief Financial Officer before retiring in mid-2015. We worked closely to transition the company from a traditional two-step distributor to a national sourcing company of kitchen and bath cabinets, decking, and other building products. This led to my being named as a finalist in 2013 for CFO of the Year by the Central Penn Business Journal.

Before that, from 1992 until 2004, I served as Controller at the York Daily Record, where I oversaw finance & accounting and human resources and participated in the sale and transfer of the company to new ownership.

I also managed information and administrative systems, among other positions, in Armstrong World Industries' Pennsylvania and Texas locations over a period of 15 years.

I believe my expansive professional experience is why I was asked to serve in this position today.

Governor Wolf understands my approach to a job like this. First and foremost, I am a citizen - a taxpayer. Like you and the citizens you represent, I want our tax dollars to be used effectively and efficiently. This is the perspective that informs my approach to this role. We plan to bring proven business practices to running an agency as complex as the Office of Administration. My early observations indicate we have the right team in place to accomplish this initiative.

I would like to provide a brief update on two major programs within the Office of Administration: our Shared Services transformation and cybersecurity.

## Shared Services

At last year's hearing, Secretary Minnich provided an overview of the goals, objectives, and approach used to execute the shared services transformation. Through this initiative, agency-run IT and HR departments under the Governor's jurisdiction were consolidated into delivery centers supporting multiple agencies with similar missions or functions. The focus was adopting a private sector approach to run IT like a business. The shared services initiative builds on decades of work to centralize and consolidate IT in the commonwealth. As a result, we have been able to:

- Eliminate redundancies to realize greater savings and efficiencies.
- Transform service delivery to allow the agencies to focus resources and funds on services to the public instead of IT operations.
- Improve the return on value of taxpayer funds through a coordinated, standardized approach to service delivery for IT services.
- Remedy inconsistent productivity and expertise in small, medium, and large agencies.
- Improve relationships and communication with stakeholders.

I am pleased to report that our efforts are working. Since 2016-17 fiscal year, we have realized $83 million in IT and HR savings through shared decision making, leveraging existing investments, and converging technology platforms.

We have also improved how agencies plan for IT projects through a new strategic planning process. We have elevated planning from the agency level to the delivery center level to focus on shared solutions to solve common challenges. We have also implemented a new governance model that gives agency leaders a greater voice in the decision-making process for strategic technology investments. The governance model is aligned with an industry standard framework and includes clear guiding principles and decision rights to ensure all stakeholders are following established processes.

OA has also transitioned to using data to run our business. We have developed and are beginning to track performance metrics to demonstrate our results such as the percentage of IT spend per agency budget, the percentage of IT projects completed on time, and the percentage of applications at risk. Some trends we have observed from this data:

1) **Less Spending** - We are spending less on information technology operations than before the shared services transformation.

2) **Fewer People** - We are managing IT in the commonwealth with a smaller IT complement than before the transformation.

3) **More Value** - We are spending less time running IT operations and more time on delivering valued projects to our customers. In reviewing our time tracking data over the past two years, we have found that our IT workforce is spending 2.8% less time on operational efforts that has transitioned to project-based work focused on growing or transforming programs that serve the citizens of Pennsylvania.

Six months ago, we issued a customer satisfaction survey to cabinet secretaries, deputy secretaries, bureau directors, division chiefs, and others to gauge how they viewed our service delivery. Overall, 85% are pleased with the IT services they are receiving.

While we recognize the significant advancement the Office of Administration has achieved through this initiative, others are taking notice as well. Last year, Pennsylvania was recognized by the National Association of State Chief Administrators (NASCA) for its IT and HR transformation.

## Cybersecurity

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.

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

- In a recent month, there were 18 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 our systems and data.

- The number of attempted hacks on commonwealth systems
  - per day: 745 million
  - per week: 5 billion
  - per month: 22 billion
  - per year: 271 billion

Over the past 12 months, approximately 289 million emails were sent to commonwealth users. Of these 289 million emails, 30 percent or 86 million were identified and blocked as spam or malicious by our email filtering service.

Other key security services we provide 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 review the code of 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 have the opportunity to 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.

This cybersecurity example illustrates how the model allows for additional standardization across the Delivery Centers, while also providing all agencies with improved resources for critical functions. It allows the Delivery Center IT staff to focus on applications to support agency programs and business functions while the enterprise resources support the technology needs to run these applications. It provides the flexibility to shift resources when work ebbs and flows based on federal, state, or other changes while incentivizing IT investments that meet multiple purposes within the established governance structure.

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.

The IRP provides a repeatable process for addressing an IT security incident. It can be modified or adapted to address the specifics of any such incident.

There is one final topic in cybersecurity we need to clarify, and that is the difference between a security incident and a data breach. A security incident is a broad term that can encompass anything from an internal human error to a coordinated external attack. A security incident could involve loss of data or disruption of service, such as a denial of service attack.

Whether or not a particular security incident results in a data breach is both a technical and legal question. With every security incident, we conduct a thorough IT forensic analysis of system logs, security monitoring tools, and other sources to determine whether any data was exposed, and, if so, what types of data were exposed, who may have seen it, and when. If data exposure occurs, we then conduct a legal analysis to determine if the incident implicates the Pennsylvania Breach of Personal Information Act, HIPAA, or any other applicable law. If the incident is considered a data breach under any of these laws, we must provide notice to those whose data was affected 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.

As we look to the future of our shared services environment, we want to optimize service delivery. This will be an ongoing activity. We currently have a portfolio of more than 2,000 applications (about 75% of them are custom-built), multiple development tools, and contracts; moving to the new model and realizing its full benefits will take several years and require approval for projects through the established governance process and structures. These decisions will continue to be made in collaboration with the agencies we serve and our Budget Office colleagues. Once approved, projects require disciplined management and commitment to successfully implement. As a point of reference, it took Michigan nearly a decade to reach a relative "end-state" in its shared services program.

That said, we must transition to the future in a way that does not impede service delivery. We are conducting ongoing portfolio reviews to manage resources, monitor service delivery, and adjust accordingly as we move forward. Our goal is to enable vital business initiatives – through automation – that deliver services to the citizens of Pennsylvania. Data modernization will eventually usher in more digital services.

We are working with agencies on several modernization initiatives including tax modernization; unemployment compensation; drivers licensing; election management; and telecommunications. Speaking of tax modernization, I would like to recognize our collaboration with the Department of Revenue team. In January of this year, we took a significant step forward with successful implementation of the initial rollout of the MyPaTH solution. It was done on time and on budget. It relied on collaboration among Department of Revenue, the Office of Administration, the Department of General Services, our agency Offices of Chief Counsel, and our suppliers. Additional phases are planned to increase efficiency and effectiveness.

With any major initiative, adjustments may be required at any point before project completion. 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.

Therefore, when considering the possibility of legislation that affects OA/OIT, we would encourage the legislature to keep this needed flexibility in mind, and to avoid legislation that is overly restrictive or requires updates to legislation on a regular basis.

As we enter 2019, the shared services initiative has matured from being a project to being our way of doing business. This is our new operating model which will continue to evolve over time. We acknowledge that work remains to fully realize all the benefits of this new approach. As we continue to improve our processes to operate as efficiently as possible, we anticipate additional opportunities to save money which will allow for reinvestment in new technology or new services. Most importantly, we will continue to focus on our obligation to taxpayers to ensure all expenditures are optimized so maximum value is provided to our customers at the lowest possible cost.

On behalf of Governor Wolf and the Office of Administration, we thank all of you who continue to support our work. We appreciate the opportunity to appear before you today. Thank you for your time.