Testimony

House Appropriations Committee

Commonwealth Informational Technology

February 27, 2018

Office of Administration

Sharon P. Minnich, Secretary

Chairman Saylor, Chairman Markosek, and Members of the Committee, I am Sharon Minnich, 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 31 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 with application development initiatives. With Pennsylvania and Ohio, he led projects related to data center consolidation, operations and standardization, increasing operational effectiveness and saving millions. He also had the chance to work with Texas and Georgia on data center outsourcing.

I am also joined by Rosa Lara, Director of the Office of Strategy and Management (OSAM); Erik Avakian, Chief Information Security Officer; and the Chief Information Officers (CIO) of our Delivery Centers (DC).

The CIOs by Delivery Center are:

- Conservation & Environment: Sean Crager
- Employment, Banking, & Revenue: Dave Naisby
- Health & Human Services: Sandy Patterson
- Public Safety: Dustin Rhoads
- General Government: Julie Snyder
- Economic Development: Phil Tomassini

I also would like to tell you a little bit about my background. I have over 20 years of experience leading major transformations and technology implementations with approximately 50% of my career in the private sector. I first worked for the commonwealth under Governor Ridge, and subsequently for Governors Schweiker, Rendell, Corbett, and now Governor Wolf. I have served as: Deputy CIO for the commonwealth; CIO of the Department of Revenue; Deputy Secretary for Financial Administration in the Office of the Budget; and Deputy Secretary for Procurement at the Department of General Services (DGS). In these roles, I improved operations and managed significant process and system changes, including the implementation of a new financial shared services model for Pennsylvania, the state's tax amnesty project, and the state's enterprise resource planning system. In addition to my work in state government, I have worked in healthcare, finance, and as a consultant in the private sector.

Before discussing specific items associated with the Office of Administration's budget, I would like to outline the major IT services that OA currently supports and the current shared service initiative that is underway. This initiative has a direct impact on the budget as presented today as well as in the future.

The Commonwealth Technology Services (CTS) line item accounts for the current services provided by OA to agencies under the Governor's jurisdiction as well as to independent boards and commissions. OA's core services include: 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, and direct service provision for network, telecommunications, data center, email, disaster recovery and continuity planning, cybersecurity, ERP, and other enterprise solutions such as the intranet & collaboration environment. These activities and the personnel and operating expenses associated with their support comprise the CTS line item in the 18-19 budget.

IT has been the role of OA since 1958 when OA implemented the first centralized computer application (payroll). As technology evolved, the services and organizational structure within OIT evolved. Up until the mid to late 1990s most agencies managed their own IT systems (applications, hardware, software, etc.) with each agency having its own IT support organization, leading to the duplication of many functions.

Beginning in the mid-1990s, OA began consolidating the commonwealth's technology infrastructure around mission-critical mainframe and server environments. As client server technology began increasing, the Enterprise Data Center was created to leverage a single facility for agency servers. Additionally, OA consolidated services for email, an enterprise resource planning system (ERP), and telecommunications networks. These early initiatives helped reduce costs; however, agency IT organizations still operated relatively independently while following OA policy and standards.

To improve oversight and coordination, in 2003 Governor Rendell issued the first Executive Order which created direct reporting relationships between the agency CIOs and the commonwealth's CIO. The intent was to provide improved oversight as IT standards became increasingly important for system interoperability, although the direct reporting requirement was limited to the CIO and not agency IT personnel.

While technology changed rapidly between 2003 and 2017, the support structure for IT remained relatively unchanged with enterprise services provided by OA and agency-specific services provided by agency IT

organizations. In response to this changing landscape, in early 2017 Governor Wolf announced the HR/IT shared services project as part of the 2017-2018 budget address. The objective was to decrease costs and improve efficiencies while also focusing on service delivery to our customers, the agencies, and citizens of Pennsylvania.

The IT shared service initiative will impact the IT financial model for the enterprise, as well as the CTS appropriation. In light of this, I would like to provide an update on the work accomplished over the past year as well as the activities in process over the next 12 to 18 months. Appendix A contains a PowerPoint outlining the initiative.

The shared services initiative is aligned to industry best practices. An August 2017 poll conducted by Government Technology Magazine found that, nationwide, more states are heading in the direction of shared services for IT with 25 states currently having some level of centralized IT functions.

Given the scope and complexity of the initiative, we are taking a phased approach to allow for a careful implementation and to reduce service delivery risk.

PLANNING AND DESIGN: JANUARY 2017-JUNE 2017

The first phase of the initiative was six months long and focused on planning and design. The project team included members from OA and agencies under the Governor's jurisdiction.

The first step in the process was analyzing the current state. At a high-level, the service delivery model in place led to both inconsistent delivery limited by personnel and funding, as well as duplication of activities given the similar IT organizational structures to support the agency business. For example, there were agencies with dedicated cyber security personnel and agencies with part-time cyber security personnel, based on resource limitations.

After reviewing the current state, the team developed the future state processes and services. We aligned processes to services and to the Information Technology Infrastructure Library (ITIL) framework, a leading industry framework for IT service delivery.

Following the development of the future state processes, the organizational structure was designed to support the service delivery model. The structure needed to support our processes and help us achieve our goals, including:

- Eliminating redundancies to realize greater savings and efficiencies.

• Transforming service delivery to allow the agencies to focus resources and funds on citizen facing activities.

• Improving the return on value of taxpayer funds through a coordinated, standardized approach to service delivery for IT services.

• Remedying inconsistent productivity and expertise in small, medium, and large agencies.

• Improving relationships and communication with stakeholders.

The basic assumption for the organizational model was to organize by service delivery area or function rather than by agency to better leverage IT assets across the enterprise. Functions that are "standard" across the enterprise were designed as part of the enterprise organizations and would serve all agencies (example: cybersecurity). Functions that are specific to agencies or lines of business would be provided by six cross-agency Delivery Centers. These Delivery Centers would be organized by IT service area and provide those services to groups of agencies.

The six cross-agency 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 previously served by OA).

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

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).

As noted under the General Government Delivery Center, we will continue to provide services to the independent boards and commissions through our data centers, network, software, technical services, and applications.

The enterprise functions include:

Strategy and Management which will establish common approaches for IT service management, IT project management, IT training, IT policy & compliance.

Enterprise Solutions will build, configure, and maintain enterprise solutions through a shared services model – enabling IT staff within the Delivery Centers to leverage solutions to further agency business missions.

Technology and Operations will provide enterprise network, telecommunication, and data center services.

Cybersecurity will protect the commonwealth's network, data, and applications from threats and attacks.

In addition to defining services and the supporting organization structure, a new governance process was designed for agency, Delivery Center, and enterprise decision making. Finally, metrics were reviewed, prioritized, and aligned to the new service delivery and governance models. The goal is to make decisions that serve multiple agencies within a Delivery Center and the enterprise.

There are two other foundational components of the model.

- **Resources** - First, to allow for flexibility and resource sharing and to serve all agencies, agency IT employees would transfer to OA's complement. The organizational model was introduced to all employees at town halls and agency meetings during the months of May and June in preparation for the July 1, 2017 employee transition.
- **Financials** - Second, a new financial model is necessary to better allocate resources.

Currently, agency IT activities are funded through a variety of mechanisms. There are enterprise billings for services such as the enterprise resource planning system, agency direct payments for consumption based services such as the data center and telecom services, direct appropriations for enterprise security, and agencies leverage federal and state funds directly for project implementation.

Staff complement are funded via the General Fund, special fund, and federal funds in any variety of ways which can limit how IT solutions are architected. In preparation for the change to the new financial model, we implemented a time tracking solution for all HR and IT employees this past July.

OA is currently working with the Office of the Budget to develop a new financial design that aligns with the shared services initiative's goals to maximize commonwealth dollars and make the most strategic IT investment decisions. The budget submittals for FY 18-19 reflect stage one of the new financial model. The increase in augmentations in the Shared Service Delivery line item reflects the costs of personnel moving from agency to OA complement.

TRANSITION: JULY 2017-JUNE 2018

The transition phase comprised governance, transition planning, and the launch of a pilot Delivery Center work stream. We took a phased organizational transition to mitigate risk and allow for additional analysis. This phase also eliminated each agency CIO and established the new Delivery Center CIO responsible for the strategic direction for all agencies within the Delivery Center.

The first activity of the Conservation & Environment Delivery Center pilot was to establish a cross-agency Delivery Center governance process. This was established in July 2017. The Delivery Center has completed transitioning its staff from their current agency structures to the new service delivery structure. Lessons learned from this transition were provided to the other Delivery Centers.

Another component of the transition phase was to establish Delivery Center Chief Technology Officers (CTO) and Information Security Officers (ISO). These changes are 90% complete. These individuals are direct reports to enterprise Cybersecurity and Technology and Operations but are physically located within their respective Delivery Center (matrixed).

Centralizing cybersecurity functions is critically important to the commonwealth. Centralization enables more efficient identification and resolution of cyber incidents, while allowing IT staff to marshal resources necessary to diagnose and mitigate a potential cyber event. Responses to a cyber event require coordination among multiple IT disciplines, systems, and vendors – having a single chain-of-command structure removes barriers to access needed information. The security backbone OIT provides is critical to protecting our resources and identifying and defending against these threats and comprised approximately 12% of the CTS budget for FY 17-18. Security

services include safeguards such as firewalls, network intrusion prevention, and blocking incoming spam, advanced malware, and virus events. The security statistics are telling:

- In a recent month, there were 7.8 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.
- Number of attempted hacks on commonwealth systems
    - per day: 216 million
    - per week: 1.5 billion
    - per month: 6.6 billion
    - per year: 80 billion

Over the past 12 months, approximately 924 million emails were sent to commonwealth users. 208 million were identified and blocked as spam or malicious by our email filtering service. Just 78% of all incoming email was considered legitimate. The other 22% (208 million messages) were blocked because they contained spam, viruses, or other malicious content.

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 before they go live on the internet. If security flaws are identified, application developers can fix the issues before the application is deployed. Based on the number of attack attempts against our internet-facing applications, this service has been instrumental in limiting the risk of a data breach.

This cyber security example illustrates how the model allows for additional standardization across agencies within the Delivery Centers, while also providing all agencies with improved resources for critical functions. It allows the Delivery Center to focus on applications or the business side of delivery while the enterprise resources assigned to the Delivery Center can support the technology needs to support those 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.

While only eight months into the initiative, several benefits have already been realized. Through consolidation into Delivery Centers, one agency with a gap

around GIS could leverage the skills and resources within the combined structure. Resource constraints for a wireless initiative in another agency were mitigated through the consolidation of personnel and sharing of resources. Through sharing of technology, an agency could implement an automated process to review and prioritize IT work that was previously done manually.

Within the pilot Delivery Center, we have also realized benefits from consolidating service desks that support agency employees. Customers now have one number to call for IT issues 24 hours a day, seven days a week. This approach is resulting in service improvements to customers that previously lacked access to a fully staffed service desk. This will serve as the model for other Delivery Centers and the enterprise.

The remaining Delivery Center teams are now implementing transition plans that depict how each Delivery Center CIO will take their organizations from the agency view to a service or functional structure, and identify resource, training, and technology gaps. The current process for agency IT strategic plans and project reviews with the Office of Budget will continue unchanged for the FY 18-19 budget and be redesigned based on the new model for the FY 19-20 budget cycle.

Delivery Center governance processes are complete and the development of service delivery metrics for each agency which will then roll up to the enterprise are on schedule for April. Based on complexity within Delivery Centers, the implementation timelines may vary to get to the final state.

EXECUTION: STABILIZATION, STANDARDIZATION & OPTIMIZATION - POST JULY 2018

As the organization begins to stabilize and the first stage of the new financial model is implemented, we will look for opportunities to prioritize areas for standardization around processes and technology. It will allow reduced business risk and improved management and oversight through both shared decision making and resource allocation. It also provides for opportunities to reduce software and hardware costs, allowing resources to be directed toward citizen focused services. For example, we are in the process of implementing a standard virtual desktop solution which will enable a remote support model for desktop support and central administration. We recently standardized on an automated server build solution that significantly reduced the time it takes to build a server from four days to one hour in one of our enterprise data centers. A few months ago, we standardized on a desktop platform for all commonwealth employees – that standardizes on a set of desktop productivity tools. These initiatives enable greater efficiencies and savings using more common technology, streamlining of training on a consistent set of

products/services and simplification of technical integrations with other back-end products.

As we look to the future, following standardization we want to optimize service delivery. This will be an ongoing activity. With a portfolio of more than 2,000 applications (about 75% of them custom-built), varying processes, multiple tools, and contracts, the movement to the new model and to realize its full benefits will take several years. The current state emerged over the last 30 years. Aligning our services to industry standards and the work completed to date has put us on the right path to implement those changes. As a point of reference, it took Michigan roughly 10 years to get to a relative "end-state" in its shared services program.

All this 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 during transition.

With any major initiative, there will be bumps in the road and it may require adjustment before there is a final end-state. More likely than not, the end-state will be different from the end-state envisioned today. That knowledge informed our decision to pilot one Delivery Center to assess and learn before moving forward with the remaining Delivery Centers.

The key is flexibility. We need the ability to modify our services and our service delivery model as the IT industry changes. Through January 2018, we have saved over $24.5 million as part of shared services through consolidation and restructuring.

With the shared service delivery model, we also expect to transform how the entire commonwealth IT enterprise functions. First, we will have a more strategic-centered model to align agency IT strategic plans to a Delivery Center IT Strategic Plan to better leverage shared resources with regard to future initiatives or investments. Second, the shared services model provides agencies with the ability to meet their objectives while also allowing them to leverage a broader network of support, thereby improving service delivery while reducing costs. Third, all agencies will have a standard level of IT which eliminates the disparity in capabilities and functions between agencies (the "have" and "have nots").

This is the beginning of the journey. While we are confident in the future direction of the delivery of IT services, we are still in the transition phase and the IT marketplace continues to change rapidly. As we transition to the new operating and funding model, we anticipate additional opportunities to save money to allow for reinvestment in new technology or new citizen services.

Thank you to all of you who have supported our work. I appreciate the opportunity to appear here today. Thank you for your time.