Testimony

Senate Communications and Technology Committee

Commonwealth Information Technology Services

SB 482

September 29, 2021

Office of Administration

John MacMillan

Commonwealth Chief Information Officer

Senator Phillips-Hill, Senator Kane, and Members of the Committee, I am John MacMillan, Chief Information Officer (CIO) for the commonwealth. You can refer to Appendix B of the written testimony for more information regarding my background.

On behalf of the Secretary of Administration (OA) Michael Newsome and OA staff, thank you for the opportunity to appear before this Committee to discuss commonwealth information technology (IT), cybersecurity, IT telework matters, and Senate Bill 482.

Although we have concerns with the bill as written, we believe we understand the intent of the legislation to make IT governance, enterprise architecture (refer to Appendix D), IT service management, and performance as effective as they can be.

Nationally, Pennsylvania is frequently recognized as a leader in information technology and cybersecurity. In the past several years, Pennsylvania has received numerous national awards including recognition by the National Association of State Chief Information Officers (NASCIO) in 2019 for our HR and IT Shared Services consolidation initiative. Refer to Appendix C for a summary of the 28 information technology and cybersecurity awards that OA has earned since 2015.

To understand information technology in the commonwealth today and our concerns with the proposed legislation, 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 cabinet level agencies. When it was originally established in 1958, OA implemented the first centralized computer application (payroll) and provided IT guidance to relevant agencies through its Bureau of Central Data Processing and the Bureau of Management Methods.

Since its inception, OA has provided services to cabinet level agencies and to select independent boards and commissions that wish to leverage our services. 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.

As technology has changed over the years, 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 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 further consolidation of IT and HR to optimize costs and improve efficiencies by focusing on service delivery. This initiative focused on the consolidation of staffing, services, and funding, coupled with the implementation of shared governance between OA and the agencies it serves. 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.

In 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 business 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.

I am pleased to say there is good news related to IT costs and what we have accomplished so far. Over the past 33 months, the new delivery model has

reduced the need for over $123 million in additional funding ("cost avoidance"). Working in partnership with the Governor's Budget Office, OA-related costs have remained flat for three consecutive fiscal years. This was accomplished 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.

In the current FY, and again in partnership with the Governor's Budget Office, we streamlined financial recoveries by merging a separate software services recovery into the shared services model. Again, keeping overall OA-related costs flat.

The commonwealth's 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, with a one team approach.

Through shared services, we have also matured the governance of IT projects. We believe that governance is the specification of the decision rights and accountability framework in the use of information technology. OA manages the supply of certain IT staff and resources while agencies generate the demands to automate their business processes. Budget constraints affect the natural intersection of the supply and demand curves. When budget is lower than the natural intersection, priorities rely on clear guiding principles. A few examples of guiding principles include reassignment of IT staff to address new legislation with time sensitive implementation requirements, accelerating digital transformation, closing business continuity gaps, and mitigating product lifecycle risks – among many others. Principles are intended to address responsibility, strategy, acquisition, performance, conformance, and human behavior.

Organizational structures, such as steering committees, facilitate the decision-making that is required to balance supply and demand constraints. Such structures evaluate, direct, and monitor the use of information technology in their organizations. Based partially on the International Standards Organization (ISO) 38500 standard, we have sought to mature the principles, architecture, business applications, IT infrastructure, and the related prioritized investments needed to successfully build and operate automated business systems. We have also aligned ourselves to industry standards for enterprise architecture maturity, a tailored version of the Federal Enterprise Architecture Framework, or FEAF, and IT service management maturity, or ITIL (IT Information Library). We are bringing proven business practices, based on industry standards, to run an agency as complex as OA. Please refer to Appendix E for more information about our governance approach.

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 innovate 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. 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.

Turning to SB 482, in October 2019, OA testified at the Senate Communications & Technology Committee hearing on SB 810, which was very similar to SB 482. The Department of General Services (DGS) also provided written testimony for that hearing. In addition, in November 2017, OA and DGS testified at the House State Government Committee hearing on HB 1704 (which again was very similar to SB 482 and the current HB 40). OA and DGS have been on record with our concerns about the bills.

The one overriding concern with SB 482 is that it is overly prescriptive with respect to commonwealth IT operations and functions. IT is a rapidly changing environment. Any organization that supports IT services must remain flexible so that it can adapt to customer needs, ever-changing technology needs and risks, and best practices in order to, inter alia, provide responsive customer service, optimize cost reduction, and appropriately utilize resources.

Two examples of OA's ability to appropriately serve the needs of our agency customers, which resulted in achieved goals with fiscal optimization, occurred in response to the passage of Act 77 of 2019 and providing support due to the pandemic. Both examples highlight the need for OA to remain flexible so that it can properly respond to requirements and needs as they arise.

Act 77 of 2019 was passed in November 2019. The capabilities required by the legislation were implemented in three-phases in December 2019, January 2020, and February 2020. To meet the scope, budget, and timeline, OA staff was re-assigned from three delivery groups to assist. By doing so, DOS avoided an unnecessary expenditure on temporary IT staff to add capacity required to complete the project within the prescribed legislative timeframes.

The following list includes examples of pandemic-related initiatives.

- Supported the transition to remote work beginning on March 16, 2020.
- Assisted with phased, data driven reopening of state offices.
- Accommodated new demands resulting directly from pandemics needs and pressures. Implemented new services and solutions quickly, several in just days.
- Maintained cyber vigilance; converged onto a single Virtual Private Network (VPN) solution.

- Established a data analytics environment for the Pandemic Recovery Team.
- Developed and implemented a Personal Protective Equipment (PPE) Donation Portal.
- Developed and implemented a Critical Medical Supplies Portal.
- Developed and implemented a Manufacturing Call to Action Portal.
- Assisted with the development and implementation of Pandemic Unemployment Assistance (PUA).
- Established a conversational virtual assistant for UC callers.
- Supported the implementation of a Business Waiver process
- Developed and implemented a Business Self Certification system.
- Assisted with the development and implementation of Encounter Notification, Bluetooth proximity solution, the COVID AlertPA mobile app.

The key is flexibility. The current IT executive order under which OA operates is written to be broad and non-prescriptive for this reason. It gives OA the authority it needs to both manage the IT enterprise and be flexible enough to address the rapid, unpredictable changes that happen in the IT world.

Executive Order 2016-6, Enterprise Information Technology (IT) Governance was first published in 2004 to establish a formal reporting relationship between agency chief information officers (CIO) and the commonwealth CIO, codify the oversight responsibility of the Office for Information Technology (OIT) for agency IT purchases and IT projects, and formally establish an IT consolidation and shared services program to realize efficiencies. The executive order was revised in 2011 based on changes in technology, IT procurement, and organizational relationships. Revisions of the executive order in 2016 reflect OIT's responsibility for security and service management, which have now become critical components of IT services in the commonwealth, as well as codify existing practices by OIT and state agencies.

Our concern is that SB 482 would undermine our ability to be nimble enough to effectively manage the commonwealth IT enterprise and cybersecurity.

SB 482 seems to place the financial burden for providing a "single point of service accessible electronically by means in use by residents of this Commonwealth" on OA. Current estimate is about $6 million per fiscal year to create the portal.

Section 4319 mandates a statewide information technology transparency portal. The bill requires that the portal list all current commonwealth IT projects. Each listing involves a summary of the project, percent of approved budget spent, original projected completion date and percentage of work completed, a summary of the scope of work, and a summary of performance requirements. The listings would be color coded green or red depending on their compliance with time, budget, and performance. "IT project" is not defined anywhere so it is unclear how a project would be summarized. The language of the bill does not sufficiently account for the wide variety of IT assets used in "IT projects" (i.e., open source vs. proprietary software, finite vs. subscription services). The red/green compliance scheme assumes fault with the contractor/provider and does not account for commonwealth caused overages such as overuse of a subscription service that bills per use rather than per user. It should be noted that the information in the project summary, scope of work, and the performance requirements may provide information to third parties regarding crucial infrastructure that may result in bad actors learning more about the commonwealth's systems than they should. Additionally, this must all be stood up within one year of the effective date of the act, which may create its own difficulties and requires funding to accomplish. Refer to Appendix A for more information.

Section 4320 mandates a process for agencies to request information technology and services. The agency must submit a business case for the IT and services. The business case must include the business reason, the method of financing, viable alternatives, and security assessment. This language presumes that the new IT Director will be qualified to make decisions on business cases from all agencies, whether the Director has any knowledge of the agencies' operations. There are no provisions for acquisition of IT or services in emergency situations that do not require the time involved in providing a business case and review. Had this provision been in place during the pandemic, it would have hindered OA's ability to support state agencies in their response to the emergencies that arose and provide services in a timely manner.

Section 4316 creates a central IT Fund from which everything related to information technology is paid. This includes IT procurements as well as IT staff salaries, and the new IT office operations budget. This section also removes the IT budgeting process from the agencies and moves it into the IT Office, under the control of the IT Director, within the Office of Administration. This language gives control of a percentage of every

agency's budget (whether the agency is under the governor's jurisdiction or not) and puts it in OA, specifically in the hands of the IT Director. This presumes an extremely high familiarity with the budgets of many diverse agencies.

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.

Unfortunately, instead of reducing costs, SB 482 will increase costs. Our estimate is that SB 482 will require between $20 and $25 million to be expended in the first year and that cost is likely to re-occur annually. Specifically, the increased cost will result from sections of SB 482 that require:

- Establishment of a single point of service portal accessible electronically by means in use by residents.
- Establishment of a formal operational testing environment to enable the rapid evaluation and introduction of new information technology services.
- Designing, developing, testing, implementing, and operating a statewide IT transparency portal.
- Performance of technical architecture reviews and capability assessments of services, technologies, and state agency systems.
- Development and implementation of efforts to standardize data elements and determine data ownership assignments (per Chief Data Officer program).
- And several other unfunded elements of SB 482.

Since OA's IT services are recovered through the shared services augmentation, the estimated costs will be additional burden to the agencies we serve. We encourage more discussion regarding the bill's design.

Since cybersecurity matters are included in SB 482 and 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 a 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. 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 38.5 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.

- From August 2020 to August 2021, the number of attempted hacks on commonwealth systems were:
    - per day: 1.2 billion
    - per week: 8.8 billion
    - per month: 38.5 billion
    - per year: 461 billion

    And include enterprise firewall, intrusion prevention system, and Internet Proxy blocked events.

Over the past 12 months approximately 815 million incoming messages arrived at our perimeter. 404 million, or 49.6%, of these incoming emails were blocked as spam or malicious by our email filtering service. Without this service, each of the users on our email platform would receive an extra 14 spam or malicious email messages every day.

Other key security services that OA provides 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, this service has been instrumental in limiting the risk of inadvertent data exposure.

During the fall of 2018, OA further formalized its 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/or the public. OA also collaborates on cybersecurity matters with the General Assembly through its IT leadership, Pennsylvania counties through our 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'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. 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. We are also helping the counties to increase their information security capabilities through the

deployment of Center for Internet Security (CIS) network security monitoring and management services through a solution referred to as Albert. Albert sensors are already deployed in 42 counties. The estimated cost to deploy sensors in the remaining 25 counties is between $400,000 and $600,000.

Albert provides network security alerts for both traditional and advanced network threats, helping organizations identify malicious activity. This cost-effective Intrusion Detection System (IDS) 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 OIT already receives alerts and notifications from the CIS SOC. A consistent approach may benefit all PA 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 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 be centralized in OA.

One example of this is the Statewide Radio Network (STARNet). The Pennsylvania State Police (PSP) has subject matter expertise with respect to public safety communications and thus, is in a better position than OA to make determinations related to many aspects of the STARNet program. SB 482 creates a "carve out" so that STARNet remains under the full control of PSP. Other agencies feel strongly that certain IT programs within those agencies should be treated in the same manner as STARNet.

The 9-1-1 program under the jurisdiction of the Pennsylvania Emergency Management Agency (PEMA) is another example of an agency with the subject matter expertise required to effectively run the program, including its activation and technology components.

However, even when a technology program and digital transformation are under the purview of an agency, OA remains available to collaborate and support. For example, OA co-chairs the Public Safety Communications Council with PSP and is supportive of the mobile radio modernization work that will protect the existing investments in STARNet and improve communication. OA also facilitates the State Geospatial Coordinating Board

established by Act 178 of 2014.

We feel that IT procurement is another function that more appropriately resides outside of OA. DGS is the agency most knowledgeable about the Procurement Code. Having procurement in DGS also provides for important separation 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. Keeping these functions separate, rather than OA doing both, allows for appropriate checks and balances and avoids potential conflicts. In conjunction with DGS, OA plays a role in shaping, evaluating, advising, and approving IT-related procurement initiatives.

OA also works with agency continuity managers to identify and implement opportunities to improve the availability and resiliency of automated business applications. Regular reviews of continuity plans for business essential systems are based on an established management directive.

With the hiring of the commonwealth's first Deputy General Counsel for Privacy, OA is now working with a dedicated expert in the Office of General Counsel regarding privacy and relevant legislation related to information technology and security.

In its current form, SB 482 takes a "one-size-fits-all" approach by consolidating IT procurement and agency programs like the ones I mentioned when they are better situated outside of OA.

The Committee also asked us to highlight some points regarding IT and telework matters. The COVID-19 pandemic was transformative with respect to telework in both the private and public sectors. One common misconception is that most commonwealth employees have been teleworking since March 2020. From the beginning of the pandemic, approximately 65% of state employees continued to report in-person full-time to their worksites. The remaining 35% of state employees either teleworked full-time or split their time between working in-person at their worksite and working remotely based on their job duties. This step was taken as an essential public health measure while at the same time ensuring essential functions of state government remained in place. For the past year and a half, telework has made it possible to achieve both goals.

Before the start of the pandemic, most commonwealth employees had never worked remotely or had limited experience in doing so. Like many other businesses and organizations, we did not have enough equipment on hand to deploy to every employee whose work location was unexpectedly closed

due to the pandemic. This created marketplace shortages for items such as laptops. Nonetheless, we assisted the agencies we support with procurement activities to acquire more than 3,100 additional laptops in the April to September 2020 timeframe. Thereafter, most acquisitions returned to established management practices for gathering demand, budgeting, acquiring, receiving, configuring, and deployment. Examples include product life cycle refresh of agency-owned devices such as desktops, laptops, and tablets. We repurposed an additional 400 existing laptops that were near end of life and helped one bureau redeploy over 650 desktops to staff working from home, among numerous other efforts. We appreciate the staff at DGS who assisted with these procurement activities.

There are many examples of how our employees have been able to telework and serve our citizens in this unprecedented and challenging COVID-19 world. OA's IT employees stood up new applications and services to support the COVID-19 response and implemented countless system changes to support operational decisions. All of this, while continuing to advance non-pandemic related projects and initiatives. We also believe our state employees have done an excellent job in ensuring the continuity of the essential functions of state government during this unprecedented time – and delivered inspired public service.

In closing, since 2017, OA has raised concerns about the IT consolidation bills introduced by the General Assembly. By doing so, we are trying to provide our IT expertise to craft and implement good policy that works for our state agencies and ultimately our citizens. We look forward to continuing a dialog on SB 482.

On behalf of 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 ***

APPENDIX A – TRACKING

OA provides information about IT projects to internal stakeholders. The information includes the status of the projects and other information for the businesses to make on-going decisions related to the projects.

Over the last thirteen months the number of OA owned, and managed servers, is near 6,300 on average, as of August 31, 2021.

OA-OIT provides central software patching services for standard device configurations. Compliance information includes updated activity for Agency-owned assets such as desktops, laptops, and tablets that are supported by OA-OIT delivery groups like C&E, EBR, GG, HHS, IED, and PS plus a few independent agencies such as SERS, Gaming Control Board, Game Commission, PUC, PENNVEST, and PMRS. In August 2021, 73,353 such devices existed in OA's view of patching targets.

APPENDIX B – STAFF PROFILES & IT POLICIES

John MacMillan was appointed Deputy Secretary for Information Technology and CIO in March 2015. He has over 35 years of experience in the IT industry. For almost 19 years, Mr. MacMillan worked for one of the world's leading IT companies. He assisted 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, he was involved in projects related to data center consolidation, operations, and standardization that achieved operational effectiveness and saved millions. Mr. MacMillan worked with customers in Texas and Georgia on data center outsourcing.

Additional information about the OA IT leadership team is available at the following link:

https://www.oa.pa.gov/Programs/Information%20Technology/Pages/leadership.aspx

Our library of IT policies is available at the following link:

https://www.oa.pa.gov/Policies/Pages/itp.aspx

APPENDIX C – AWARD SUMMARY

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

Year	Organization	Description
2021	NASCIO	Finalist, 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

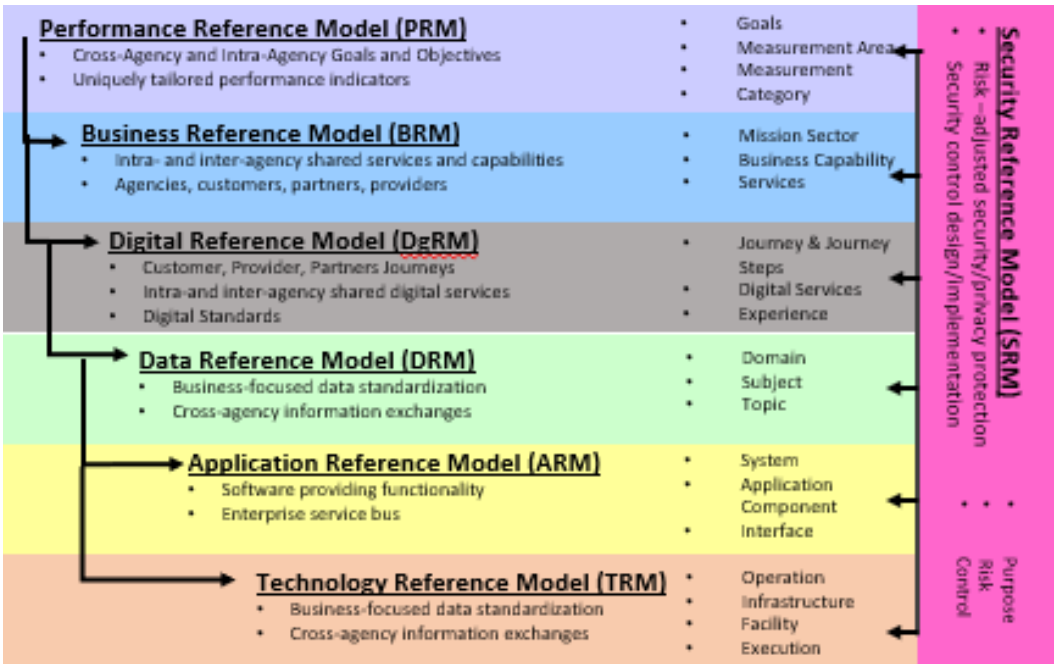
APPENDIX D - ARCHITECTURE

Enterprise Architecture (EA) supports planning and decision-making through documentation and information that provides an abstracted view of an enterprise at various levels of scope and detail. In late 2018, OA adopted the use, and seeks to mature, a tailored version of the Federal Enterprise Architecture Framework, or FEAF.

At its core is the Consolidated Reference Model (CRM), which equips agencies with a common language and framework to describe and analyze investments. The CRM consists of a set of interrelated "reference models" that describe the seven sub-architecture domains in the framework:

1. Strategy
2. Business
3. Digital [*added by OA*]
4. Data
5. Applications
6. Infrastructure
7. Security

These individual reference models are designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across agencies. The following graphic depicts our tailoring of the FEAF CRM.

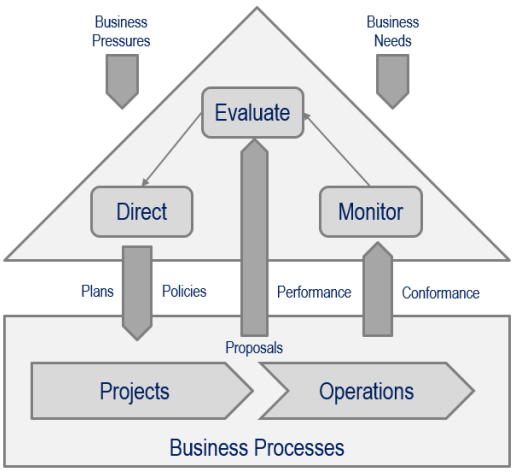


APPENDIX E – IT GOVERNANCE

Based partially on the International Standards Organization (ISO) 38500 standard, OA has sought to mature the principles, architecture, business applications, IT infrastructure and the related prioritized investments needed to successfully build and operate automated business systems. The following graphic summarizes the components.

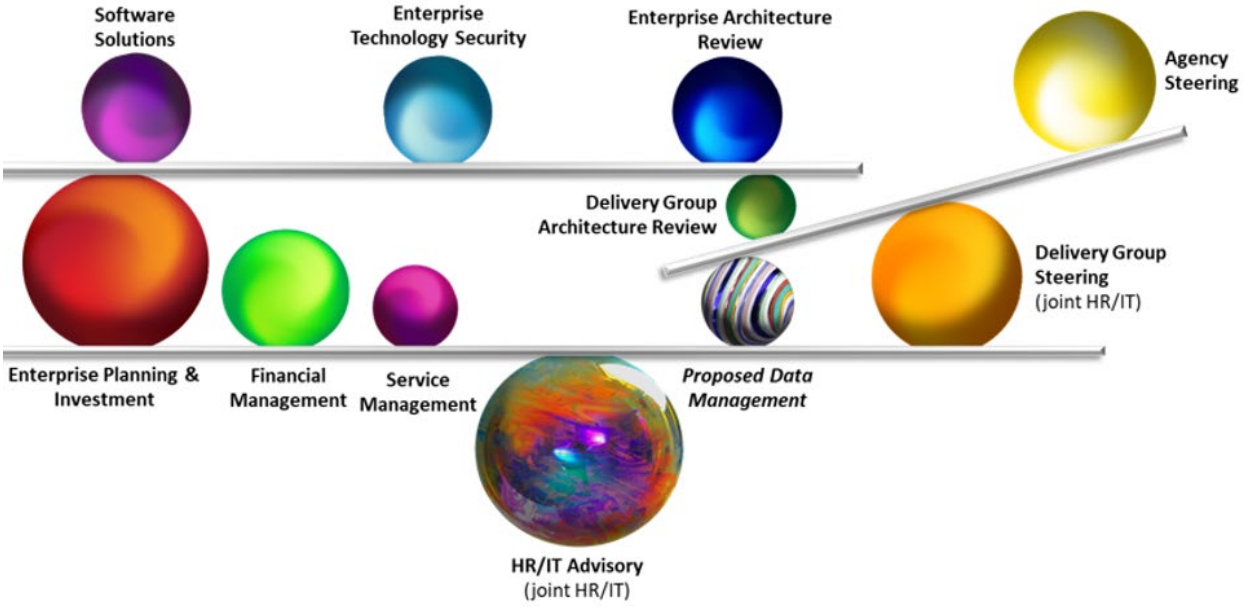
<table>
<tr><td colspan="3">IT Principles
High level statements about how IT is used in the organization</td></tr>
<tr><td rowspan="2">IT Architecture
Organizing logic for data, applications and infrastructure captured in a set of policies, relationships and technical choices to achieve desired business and technical standardization and integration.</td><td>Business Applications
Specifying the business need for purchased or internally developed IT applications.</td><td rowspan="2">IT Investment and Prioritization
Decisions about how much, where to invest, when to invest in IT, including project approvals and justification techniques.</td></tr>
<tr><td>IT Infrastructure
Centrally coordinated, shared IT services that provide the foundation for the organization's IT capability.</td></tr>
</table>

ISO 38500 provide a consistent framework for governing bodies to use when evaluating, directing, and monitoring the use of information technology (IT) in their organizations. The graphic to the right provides an overview. Evaluating, directing, and monitoring projects relies on clear guiding principles. Principles are structured to address responsibility, strategy, acquisition, performance, conformance, and human behavior.



Organizational structures, such as steering committees, are needed to facilitate decision-making that is required to balance supply and demand constraints. Such groups develop and promote collaborative decision-making, shared accountability, and incremental innovation to encourage desirable behavior. The following graphic provides a depiction of established and potential groups that form

the IT governance structures. Note that the graphic attempts to balance business pressures and needs while provide an escalation path from individual agency relationships to deliver groups to cabinet-level HR/IT Advisory.



Operating Concept documents provide members of the governing structures with narrative guidance for:

- Evaluating proposals
- Establishing strategies, policies and continuously monitor:
    - Implementation activities and status
    - Performance
    - Conformance
- Balancing supply of and demand for resources