UNISYS | Securing Your Tomorrow®

Hearing on SB 810, PN 1117

Testimony by
John Alwine
Unisys Public Sector, Region Director – Commonwealth of Pennsylvania

Before the
Senate Communications & Technology Committee
Pennsylvania Senate

October 30, 2019

The Honorable Kristin Phillips-Hill, Chairman

Chairman Phillips-Hill, Minority Chair Santarsiero and members of the Senate Communications & Technology Committee, thank you for the invitation to testify before you on behalf of Unisys regarding Senate Bill 810, PN 1117. We believe this legislation is critical to helping move Pennsylvania forward to the forefront of information technology efforts. We strongly support the effort to enhance the Commonwealth operating in a coordinated, transparent manner, driving procurement efforts that better provide value to agencies and tax payers and protecting critical data through strong cybersecurity efforts.

My testimony will focus on helping identify the right level of independent oversight and accountability for delivering results for the Commonwealth as it relates to the use of information technology (IT) in state government. IT is no longer solely an administrative function; it has become a critical component – costing nearly $1 billion annually in Pennsylvania – for states to successfully perform their core missions. I plan to speak on three general topics within this legislation. The first is discussing the Director/CIO position, an increasingly critical position in all states, not just the Commonwealth. Senate Bill 810 is an opportunity to build into the job description qualities - beyond just knowledge of technology – which will help position future job holders for success. Second, I will also discuss how the Commonwealth can best support individual agencies working in coordination with the Office and Director to identify IT needs and achieve desired outcomes. Finally, I will reflect on the creation of a Joint Cybersecurity Task Force, and the additional elements we believe would strengthen its desired outcomes. My comments reflect best practices across other states and the federal government and leverage my own experiences as well as extensive expertise by individuals within Unisys.

About Unisys

My name is John Alwine and I serve as Unisys' Region Director for Pennsylvania as well as being a life-long resident of the Commonwealth, having grown up in Dauphin County and graduating from Shippensburg University. Unisys is a global technology leader with headquarters in Blue Bell, Pennsylvania,

that builds high-performance, security-centric solutions for the most demanding businesses and governments. We provide services to over two dozen states with offerings that include security solutions, advanced data analytics, cloud and infrastructure services, application services, and application and server software. We have a strong focus on digital government and specialized expertise in leading practices across public sector entities.

More importantly, we are a company rooted here in Philadelphia, Pennsylvania. It is where we developed the world's first commercially available computer system in collaboration with the University of Pennsylvania in 1945. Unisys is proud to be a trusted advisor and supplier of IT services to Pennsylvania; the Commonwealth's largest information technology partner. For decades, Unisys has successfully collaborated with the Commonwealth to provide reliable, cost-effective and mission critical services to Pennsylvania government agencies and citizens. Unisys' digital services have streamlined state operations, saved taxpayers millions of dollars, ensured public safety, and improved the ability of Pennsylvania citizens to obtain online access to valuable information and government services.

In June 2014, Unisys and the Commonwealth launched a first-of-its-kind initiative that transformed how state agencies acquire IT services. Through this initiative, called Pennsylvania Compute Services, or PACS, Unisys invested $77M and is providing and operating one of the largest, Criminal Justice Information Security (CJIS) protocol secure, private cloud-based, on-demand IT computing implementations by a state government. Under the competitively-awarded PACS contract, Unisys consolidated data centers into a secure private hybrid cloud that enables agencies to access IT services as needed, protecting the citizens' data while enhancing flexibility and service delivery available to more than 45 state agencies, boards and commissions.

It is safe to say our experience in the Commonwealth and across the country has enabled us to understand best practices for states' IT operations and procurement. These best practices help drive better understanding of IT needs, greater coordination and cooperation amongst state entities and between the public and private sector, and efforts that enhance the value IT procurement can deliver while doing so in a manner that reduces risk.

We believe that with changes to the language creating a new director and additional clarification on transparency, accountability and cybersecurity, this legislation will help drive greater success in the Commonwealth's information technology efforts while promoting more efficient use of taxpayer dollars and protection of critical information.

Information Technology as a path to digital modernization

Unisys understands that information technology has become more complex over the past few decades. State governments have struggled to react, often because of difficulty in adopting to emerging technologies, overcoming procurement requirements designed for defined items such as keyboards or printers and hiring and retaining internal personnel with the skillset to best leverage new tools and

expectations. None of these issues is unique to Pennsylvania; these are challenges Unisys has witnessed across the country. States are adopting to the idea that information technology is tightly coupled into key operational processes, from residents applying to vote to figuring out whether someone stopped by police for speeding is a criminal who just escaped from prison

The Commonwealth needs to develop a strategy and roadmap that guides agencies in how to best leverage new technologies, or risk excess IT spending, cyber security issues that threaten critical data – including citizen information - and poor performing projects. Currently, and across multiple Administrations, IT spending has frequently been done in an ad hoc, uncoordinated manner with minimal oversight and accountability when goals and objectives were not achieved. This had led to projects without clear objectives, costs overruns, missed opportunities to capitalize on innovation and the inability to make measurable progress in modernizing government operations.

IT is no longer about the newest computer or best mouse and keyboard; it is not about hardware but instead about meeting increasingly complex agency needs while securing significant amounts of data. The ability of government to benefit from today's innovation depends on having the right management structure —do executives have real data on the cost to deliver IT today? Do they know what are (and how to mitigate) risks such as cybersecurity? Do they have a way to map the opportunities for automation, mobility, and data analytics to agency business processes so that services are better and more efficient for the citizens and businesses of Pennsylvania? Is there a mechanism to both incentivize and hold the right people accountable for delivering on those opportunities?

The Commonwealth's IT should feature a governance structure that allows for the effective management of IT and decision making process, an understanding of the real cost to deliver internal IT as a service today, and avoids disjointed efforts to map the business process which runs on the applications and infrastructure currently utilized by the Commonwealth today.

We agree with SB 810's findings that continuing down the path of digital modernization and addressing increasing risk concerns will lead to better use of data, better customer (resident) service, greater protection from security risks and increased savings for the agencies and ultimately the tax payer.

Successful digital modernization though depends on three ideas: (1) Providing a balance of power and accountability between a modern, qualified IT leader and internal clients, the agencies, (2) Picking the right mix of technology opportunities so as to balance innovation with key IT risks and (3) a commitment to a strong cybersecurity program and oversight effort. The success of each of these is augmented by a positive and cooperative relationship between the public and private sector. These overarching goals are predicated on the need for the Commonwealth's IT leadership to implement a clear and transparent plan based on measurable objectives... It requires strategic, accountable leadership responsible for coordinating decision-making but able to step in and stop individual projects that may not be performing to expectation. In today's shift from IT as a capital expenditure to IT-as-a-Service, the model must include a framework for the public and private sector to partner in developing

innovative solutions to ideas that government may not yet even have considered. And that involves frequent, effective coordination between IT leaders, individual agencies and the private sector to identify technology needs and achieve desired outcomes.

The Chief Information Officer - providing a balance of authority and accountability between a modern, qualified CIO and internal agency clients

The role of Chief Information Officer / Director of an Officer of Information Technology (CIO) is quickly changing as innovative states move away from owning hardware and doing everything internally, and instead are now turning to procuring services on demand (data center as a service; security as a service, other) and working closer and cooperatively with the private sector to meet the increasing needs and risks. It is the appointment and accountability for the bill's director and their ability to meet this changing environment that gives us the greatest pause.

As currently drafted in §4313, the Secretary of the Office of Administration appoints the director, whose only qualification is five years of experience dealing *"with public sector information systems in a State government agency or an equivalent entity. The qualifications shall include, but are not limited to, verifying that an individual has the proper industry certifications necessary to perform the duties under this chapter."* The bill would create the Office of Information Technology and empower its director with broad powers concerning the state's IT, including supervision and management of the procurement of all information technology services; establishment of standards and policies for IT procurement and cybersecurity and; oversight and management all state agency contracts regarding IT. Finding one individual with the ability and knowledge to handle this much authority is extraordinarily challenging.

In an environment demanding knowledge and skills covering not only technology but public administration, acquisition and finance, the current language is limited in its focus. Given that IT spending in the Commonwealth is more than $1B annually and all resources and personnel now report directly to the CIO, vesting too much authority in one individual without a clear set of objectives and accountability structure is an inherently risky way to ensure alignment to the goals of the legislation. As we have observed in other states, we believe that the Commonwealth would be best served by an individual with a strong, diverse background in the skills mentioned above, along with the ability to work well in conjunction with all involved stakeholders – public and private sector - to be positioned for success in driving the Commonwealth's IT initiatives.

In my experience, states have not used a formal sounding board to help identify prospective CIO candidates. Too often, a Governor or senior staff defer to agency recommendations regarding the CIO. While this is typical of how most states operate, it does not always result in the best qualified and capable individual for the CIO position. Pennsylvania, through this legislation, has the opportunity to demonstrate its recognition of the importance of the CIO position and set the bar above its peers in choosing future leaders for the Commonwealth's IT efforts.

We would suggest inclusion of language based on one of two models. The first is the Pennsylvania Model for judicial selection which is drawn from the State Bar Association's review of all judicial candidates. Under this method, the Governor would submit a list of candidates to an entity, for example the County Commissioner Association of Pennsylvania's Technology Committee**,** which would then vet the pool and publically share the ratings. The Governor would then be free to make a better informed selection, relying on those ratings in the decision-making process. This method provides an independent, non-partisan source of information to the Governor from experts in the industry without unduly restricting the Governor or his Secretary's appointment authority.

The alternative option we recommend is based on the Florida Judicial Nominating process. When there is a judicial vacancy, the Governor requests the Chair of the Judicial Nominating Committee (JNC) to convene the Committee for the purpose of selecting and submitting names of qualified individuals to the Governor for appointment. The JNC investigates each applicant to confirm eligibility and then interviews them before voting on which applicants (usually 3-6 candidates) to recommend to the Governor. The Governor then appoints a judge from among the nominees. This is meant to help push forward qualified candidates. In a similar manner, given both the importance and highly sophisticated nature of IT, language could be written to create a CIO Nominating Committee that would play the same role. As above, while the Governor retains complete appointment power, the pool of candidates would be pre-judged to have the necessary skillsets to thrive in the role. Either model increases the probability that a person would be selected on the merits, with the help of those who understand the specialized needs and requirements of the CIO position.

We would also recommend adding language to create a private sector advisory board. In today's fast moving technological environment where quantum computing and artificial intelligence are being adopted by states and the private sector and not just science fiction concepts, presuming that any one government official will have the latest insight on technology trends across the country or globe that could impact or aid the Commonwealth is unlikely. In the past, some CIOs have utilized a private sector advisory board to provide feedback and insight as well as critical evaluation on technology strategy and tactics. To the best of my knowledge, this advisory system has not been utilized by recent Administrations. At the state and municipal level, Nevada created the Information Technology Advisory Board by statute; Oregon established the E-Government Portal Advisory Board; and the City of Atlanta recently created a CIO Advisory Board. At the federal level multiple agencies have utilized private sector advisory boards or project-specific groups providing critical knowledge and feedback to improve government initiatives. Why shouldn't Pennsylvania enjoy a similar system and tap into the knowledge and views of its own corporate citizens?

We support the current legislative language in §4315 requiring the director to coordinate with individual agencies to develop IT plans and policies. Unisys believes that without frequent coordination and communication between the CIO and the end-user agencies, projects cannot be successfully identified, developed and implemented.

Coordination to promote success - picking the right mix of technology opportunities so as to balance innovation with key IT risks, including project management and contracting

In our experience in many states, we see IT decisions made in a black hole with limited communication and feedback around transformational plans or strategic priorities shared between centralized information officers and agency IT leaders.

Likewise, there is value in providing the vendor community access to the Commonwealth's operational plans where they may be able to suggest better ways to achieve desired outcomes or, at a minimum, be able to put context around why certain activities are occurring. Lack of transparency provides the perception that decisions are impromptu without thoughtful consideration.

When there is an inability to clearly lay out and follow a strategic plan, we have seen state agencies unable to adjust their IT needs and strategy in a cohesive manner to fit the overall objectives of the state.

The language in Senate Bill 810 §4320 establishes a federated governance framework where individual agencies work in coordination with the Office and Director to identify IT needs and achieve desired outcomes. To request IT services, Commonwealth agencies must first set out their requirements within a business case with defined information. The Director is then responsible and accountable for meeting agency needs in a secure, cost-effective manner using shared services and other modern IT solutions such as cloud computing. We support this and believe that the coordination of agencies identifying needs and working with the Director and Office will lead to the enhanced use of technology to develop innovative policy solutions.

By establishing an upfront description of projects and their solutions, issues can be identified relative to the underlying business case metrics relatively quicker. Once identified, the bill establishes a framework in §4321 for rapidly addressing problems while limiting potential cost overruns by ending future expenditures. The legislative language adds another layer of accountability and transparency for all major IT projects by introducing a public internet portal. Taxpayers, the General Assembly, agencies and all stakeholders will be able to view regularly updated information regarding public IT expenditures, IT policies, cybersecurity posture, and IT project results. We would recommend that the Commonwealth's IT operational plans along with specific objectives to be achieved and timeline for completion also be made available for public view on the portal. The inclusion of this information in such a manner will expand the Commonwealth's ability to share data with the public while providing more transparency in the role of IT in government services.

We recognize that the legislative language is based on the COBIT *(Control Objectives for Information and related Technology)* IT management and governance framework successfully implemented by many large government and commercial organizations. As a large vendor at that level, we have seen the COBIT Framework used to identify a set of practices for how an organization improves maturity of IT management by focusing on effective planning, organization of roles and responsibilities,

acquisition, implementation, operations, measurement and continuous improvement. Like other government and commercial organizations that have used the COBIT Framework, effective use will enable the Commonwealth to better align IT activities to agency mission objectives while preventing, detecting and mitigating risks.

The legislation concentrates development of workforce expertise to improve IT results by better aligning roles, responsibilities and accountabilities. It requires the Office to identify opportunities in IT trends and consider how to apply those trends for the benefit of the Commonwealth and its agencies. In creating and maintaining the strategic IT plan, the Director must outline a comprehensive government-wide approach for getting the most value from IT spending, while protecting security and privacy. It establishes clear measures of performance and implements a transparent accountability framework that highlights issues and requires the Commonwealth leadership to rapidly resolve risks.

Unisys would recommend changing the required annual strategic plan in §4311 to a three (3) year plan, similar to the method in a number of states including Kansas and North Carolina. Alternatively, we would suggest a 3-year strategic plan with annual updates. A one-year plan can be restrictive and limit the ability of the director and agencies to plan outwards, knowing that technology changes can take multiple years to fully adopt and implement

The Joint Cybersecurity Task Force - strengthening the Commonwealth's cybersecurity efforts

Unisys would also like to address concerns within sections of the bill tied to cybersecurity. In an area of increasing importance in today's world, we would like to share our experience currently dealing with the issue for the Commonwealth, as well as our knowledge from other state and global clients to offer a different way to think about meeting cybersecurity challenges the state faces today and will face tomorrow.

We applaud legislators for creating a Joint Cybersecurity Oversight Committee that includes not only representatives from the Commonwealth but private sector cybersecurity experts as well. Leveraging the knowledge and skillset of the private sector enables the Commonwealth to benefit from a broader base of experience and information that will only lead to smarter, more informed decision-making.

Regarding the Committee makeup, while the Committee would enjoy a wealth of representation from law enforcement, including the Attorney General and State Police, we do question the inclusion of a member of the National Guard. Unnecessary representatives from law enforcement may be a cause of concern for the general public and privacy advocates.

By establishing in §4354 the Committee as reviewing and coordinating cybersecurity policies as well as discussing emerging threats, the Commonwealth is taking a proactive step similar to what we have seen in other states. Connecticut and Florida are two recent examples of states establishing cybersecurity Task Forces to confront what has become an overwhelming threat to the security and reliability of government operations and data.

Having experienced the potential scope of this threat through the services we provide in other states, we would like to suggest potential changes to the current legislative language that we feel will enhance the goals of this provision.

In reviewing and coordinating cybersecurity policies, there is no language to transmit those recommendations to the agencies or other arms of the government for their consideration. Further, there is no requirement for agencies and government entities to adopt or even comment on those recommendations. We have found that when cybersecurity is left to each agency, its response will often be determined by the budget dollars available. If this Committee is to have its strongest impact, we recommend a requirement that any policy recommendations made be transmitted to all applicable government agencies along with specific follow up and assessment on the adoption of said policies.

We also note that the language in §4354(g) only requires the Committee to prepare a single report of its activities. We would recommend this be changed to an annual report, recognizing that cybersecurity threats are frequently changing, requiring constant vigilance and attention.

Conclusion

Unisys supports SB 810, PN 1117 as a means to modernize the Commonwealth's information technology governance, procurement and interoperability through increased transparency, accountability and coordination. As drafted, this legislation will drive increased coordination amongst state IT users, foster accountability in the development and use of IT within the state and drive down costs while increasing recognition of security risks for state agencies.

I would be remiss if I failed to mention that to achieve the greatest return, the legislature and Judiciary should ultimately work with the director to include their systems under the same review, protection and oversight umbrella as those mandated for agencies under this legislation. Though independent entities, each part of our government is vulnerable and should be considered pieces of a greater whole, rather than as three distinct and unique technology systems.

Like most states, the Commonwealth faces a continuing challenge to maintain and improve the quality of services it provides, while dealing with an ever-changing technology environment. Pennsylvania must continue to take important steps to reduce barriers to success by fostering an environment in which a skilled technology leader is allowed to coordinate with agency IT officials to innovate and develop the next generation of digital government technology. Supported by, and working cooperatively with, a private sector that can provide insight and feedback on the Commonwealth's strategic and tactical vision, this legislation will help push Pennsylvania to the forefront of state government IT efforts.

To these ends, Unisys is pleased to offer our thoughts, and appreciates the recommendations made by others testifying before your Committee. We look forward to continuing to work with the legislature

and the Administration to address these important issues and to find new ways to allow the state to take advantage of technological innovations that produce better results at a lower cost and in a more secure manner for agencies and residents. Thank you for the opportunity to testify and to share our views, and I welcome any questions you may have.