**Hearing on Cybersecurity**

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

**Before the Majority Policy Committee**
**Pennsylvania House of Representatives**

**March 28, 2022**

**The Honorable Martin Causer, Chairman**

Chairman Causer and members of the Majority Policy Committee, thank you for the invitation to testify before you on behalf of Unisys regarding cybersecurity. It is Unisys' position that while many large businesses and various industries have been focused on their own security and defensive measures over the past decade, to varying degrees of success, the public sector has been too slow to realize the significant threat to their own critical systems and information. Whether it be protecting personally identifiable information such as tax records, unemployment claims or social security numbers, or the systems that allow the Commonwealth to administer licenses, distribute unemployment checks or collect tax receipts, for too long government has utilized outdated approaches to secure their most important assets. Unisys believes that taking critical steps towards supporting and enhancing the Commonwealth's security environment will mitigate risk to continued operation and bolster public trust and the reputation of the Commonwealth's government entities.

My testimony will provide a measured approach, recognizing that the Commonwealth does not have unlimited financial resources to put towards cybersecurity, nor does it have the extensive staffing support necessary to carry out all recommendations internally. Within the time constraints of this hearing, it will not be possible to go beyond our initial set of recommendations, but I will highlight four actions that I believe will support ongoing Commonwealth activity while also putting Pennsylvania farther down the road to a stronger security posture.

My testimony will focus on helping identify the right actions for delivering results for the Commonwealth as it relates to protecting critical data and systems via the use of information technology (IT) in state government. 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.

I hope by the end to have shared critical information that both informs this committee and provides a potential roadmap that, when done in coordination with the Commonwealth's IT leaders, produces a safer and more secure operational environment.

**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, including security operations.

More importantly, we are a company rooted 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, including their security posture. These best practices help drive better understanding of IT security needs, the need for greater coordination and cooperation amongst state entities and between the public and private sector, and efforts that protect critical systems and data in a cost-effective and efficient manner.

We believe that the Commonwealth can take specific actions to enhance their security posture at a time when the public sector faces more extensive cybersecurity risks than ever before.

## Current World Affairs Are Accelerating The Security Risk to Critical Entities

Verizon's 2019 Data Breach Investigations Report reported that public sector organizations were involved in one-in-five cyber incidents, amounting to over 3,000 cyberattacks. Their data also revealed that approximately 47% of public sector data breaches were not discovered until years after the initial attack. This delayed discovery allows criminals more time to steal information and wreak havoc while avoiding detection and responsibility for their crimes.

Three years later and the world has not gotten safer. The Russian invasion of Ukraine has prompted increased concerns over wide spread national-state cyber-attacks. According to a report published earlier this month by cybersecurity firm Mandiant, a Chinese state-sponsored hacking group successfully compromised the computer networks of at least six U.S. state governments between May 2021 and February 2022.

On top of international affairs, the pandemic has had, and will continue to have, an impact on security needs as the Commonwealth and other states accelerate their digital transformation efforts to meet a new operating involvement. No longer are all employees expected to be in one state-owned location all the time. The work from home / hybrid work approach brings with its new demands, as do initiatives to move data and operations to a cloud environment.

The risk to any individual or organization, private or public sector, has never been greater. No longer are private sector entities the sole target for cyberattacks; state and federal government agencies, departments and educational institutions are making up a growing proportion of all attacks. The reputational and economic exposure has grown exponentially in response to world affairs, and many individuals and organizations – including the Commonwealth - are inadequately prepared for the consequences of the severity of the possible negative outcomes. News reports of breaches have become a near daily occurrence. Most of us have been issued new bank cards at one time or another well in advance of the expiration dates as a response to some of these breaches. Worse yet, when protected or private personal data is shared because it can be, not because it should be, the opportunity for misuse escalates, along with the risk of reputational damage and of course the potential for litigation. It is critical that public and private sector entities take a collaborative approach to security, leveraging each other's strengths and abilities to increase the security of critical systems and data.

## Security Approach of the Commonwealth's Peers

Cybersecurity is no longer a challenge to be met from whatever remains of an agencies' information technology budget. As recently as 2020, fewer than 40% of states had a dedicated budget line item for cybersecurity, and half of states were allocating less than 3% of their total IT budget to cybersecurity. That approach has begun changing, driven as I mentioned, by global events, but in no way has state spending reached what most cybersecurity experts would say is a satisfactory level. According to the

2022 Public Sector Cybersecurity Survey Report by SolarWinds, 50% of state government respondents and 25% of local governments indicated that budget constraints are an obstacle to maintaining or improving IT security.

The federal government has either given states and localities flexibility to spend federal recovery dollars on cybersecurity initiatives (CARES Act) or directly appropriated funds for use to meet rising cyber challenges (ARPA). In the Infrastructure and Investment Jobs Act, passed late last year, the federal government designated over $2 billion in funding for cybersecurity resiliency and innovation. The bill includes funds to reduce cyber vulnerabilities in public water systems and drinking/clean water technology. Additionally, the bill allocates state and local funding via grant programs for cyber functions to include detecting and recovering from cyber threats and emergencies. The law requires states to create cybersecurity plans in order to receive grants.

At the state level, legislators are including specific line items to support cybersecurity efforts. Some recent examples of states appropriation dollars specifically for cybersecurity initiatives:

- Florida will provide $87+M to fortify cybersecurity in the state, including $50M to "Enterprise Cybersecurity Resiliency".
- The Virginia House of Delegates submitted its version of the state's budget, allocating $150 million for cybersecurity initiatives for the next two years
- Texas created a Technology Improvement and Modernization Fund to improve state agency information resources, with $898.6M to support state cybersecurity and legacy system projects.
  Maine appropriated state and federal recovery funds to tackle the highest-cyber risk areas identified by an external program review, including formalizing a business continuity plan for the State's information technology, as well as other identified cybersecurity programs.

Additionally, states such as Minnesota, Montana and Washington included specific cybersecurity initiatives in their budgets as a means to focus their own state's IT agencies on cybersecurity initiatives rather than leaving all funding in one large IT pot.

It is imperative that states, including the Commonwealth, provide necessary funds to support improvements in their security posture or their reputational, operational and legal implications will continue to increase.

**The Commonwealth's Current Security Structure**

Governor's Office of Administration (OA) Enterprise Information Security Office (EISO) is responsible for the overall security posture for the agencies, departments, offices and other organizations within the Governor's jurisdiction. For management purposes, these organizations – about 50 overall – are aligned under six delivery centers organized according to business type, e.g. Corrections and State Police are grouped together in the Public Safety Delivery Center.

The Commonwealth has both a Deputy Secretary for Information Technology (who also serves as the state Chief Information Officer) and a Chief Information Security Officer (CISO). While the CIO has overall responsibility for information technology and security vision and strategy for the Commonwealth, the CISO is generally responsible for security strategy, policy, planning, execution and reporting. The CIO and CISO and their teams are responsible for thousands of applications, multiple data centers, cloud services, hundreds of remote facilities, dozens of standards and policies, hundreds of suppliers, and service for many customers, including 90,000 employees and contractors and 12 million citizens. The organization is also responsible for implementing the relevant legislative initiatives, including legislation affecting cybersecurity requirements.

Recent legislation has attempted to address components of security, including ransomware attacks (SB 726), creation of a joint cybersecurity committee (SB 482) and data breaches (SB 696), but Pennsylvania has not appropriated any budget dollars specifically to cybersecurity efforts in a manner similar to some of her peer states. In summary, the security organization is small and has what we believe is insufficient direct financial appropriations with respect to its core mission of managing security and risk for the Commonwealth overall.

**Recommendations to Move the Commonwealth to a More Secure Governance Structure**

Quickly transitioning from a state of vulnerability to a locked down environment where cyber-attacks are addressed in a timely manner and damage is minimalized (because attacks will never be 100% prevented), is not something that can be accomplished overnight.

Unisys understands that cybersecurity and information technology has become more complex since the start of the pandemic, let alone over the past decade. 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 security must be addressed in a holistic, whole-of-government approach. As such, we would recommend the following four actions to help the Commonwealth identify its risk profile, understand how to most efficiently utilize available funding to maximize return (protection) and make significant strides towards a stronger security framework. The four steps are:

1. Establish a strategic governance and architecture of ZeroTrust cybersecurity services to define the target state, leveraging best practices for all corporations and government.
2. Provide overall risk profile of current security environment and a strategic plan to make further investments that maximize appropriated funds.
3. Create a reliable data backup and recovery platform designed to mitigate the impact of ransomware attacks.

4. Modernize identity and access management that supports citizen digital services and improves workforce access while providing secure access control and authentication.

IT is no longer about the newest firewall, adopting the latest virtual private network trend or signing up for security tools without having the ability to successfully manage their adoption; it is instead about meeting increasingly complex agency needs while securing significant amounts of data.

**Establishing ZeroTrust**

It establishes the thinking and actions through-out Commonwealth employees where trust is never granted implicitly to the users of the systems, but must be continually evaluated. The purchased solution would make core agency's citizens service environment more resilient and secure while facilitating improved access to government services, reducing the cost of compliancy and reducing long-term capital expenditures.

Adoption of a zero-trust approach is becoming a fundamental tenant for cybersecurity efforts. The following steps are essential to reaching a zero-trust security model:

- Prioritize cybersecurity investments based on their business impact
- Protect people, devices, networks and data from attack
- Predict threats and cyber risks by continuously monitoring traffic and automating detection using predictive artificial intelligence driven technology
- Isolate advanced persistent threats quickly and effectively reducing impact to critical data and systems
- Remediate operational impact of attacks by reducing response time

In 2020, the Federal Bureau of Investigation's Internet Crime Center (IC3) received a record-breaking 791,790 cybercrime complaints, with reported losses of $4.2 billion. In addition, the Cybersecurity Workforce Study reported in 2021 that there is still a need for over 2.7 million cybersecurity specialists. As the demand continues for improved digital services that can drive operational efficiencies and improved customer service, enhanced cybersecurity capabilities will be critical to the delivery of trusted and reliable government services.

Establishing a ZeroTrust environment is the foundation to improved cybersecurity efforts, focused on protecting an enterprise's most critical asset: data. This can be accomplished by using encryption and by limiting and controlling access. Both approaches are enabled and enhanced by implementing ZeroTrust cybersecurity architectures that, unlike perimeter-style defenses that only see the outside world as a threat, work by assuming all network traffic is suspect and cannot be trusted. Establishing the strategic governance and architecture of these services provide for a solid cybersecurity foundation that minimizes risk for the Commonwealth, thereby defining a strategic approach to procurement of supporting infrastructure, not buying stand-alone "things" such as new hardware devices.

**Provide overall risk profile of current security environment**

Cybersecurity risk continues to be a significant concern for state government. It is again the number one priority on the 2022 NASCIO CIO Top 10 Priorities. However, it remains difficult to understand and communicate this risk in financial terms that promote informed decisions on effective use of budget dollars. The result is a disconnect that leaves agencies and departments with unknown risk exposure and an inability to properly manage and remediate their cyber risk. Services are available to provide an overall RISK profile of the current security environment and a strategic plan to make further investments that will maximize funding usage. These services provide executives a dashboard, proactively demonstrating the cost in real dollars of a potential ransomware attack. This provides understanding of current spend to better allocate budgets in a "what if" analysis, planning and reducing risk to the business and also identifying potential gaps that may exist today.

Organizations such as the Commonwealth need to be aware of the true level of their own economic exposure from cyberattack, Sufficient resources can best be made available to solve issues when this risk is credibly quantified and the return on investment is more clearly understood. Effective methods to quantify this risk exist, and establishing this discipline with any organization is highly encouraged. If Equifax had known that the cost of their 2017 breach would exceed $1.3 Billion, they would have likely insured themselves for more than just a tenth of that amount and established greater rigor and posture.

Cyber-risk management tools can enable the Commonwealth Chief Security Officer to:

- Assess cybersecurity and cyber risk posture in economic terms.
- Understand where the risk transfer zone is for all cyber perils.
- Easily communicate risk reduction initiatives to the Commonwealth Leadership.
- Prioritize risk mitigation strategies.
- Analyze the return on investment of cybersecurity investments.
- Determine the likelihood of a cyber-related financial loss.

Risk mitigation efforts are becoming increasingly more important as entities can no longer rely on cyber-insurance as a cost effective or efficient use of financial resources. For instance, the Local Government Insurance Trust, a member-owned association that offers pooled insurance to 191 Maryland municipalities, reported a 300% increase for 2022 cyber insurance. CompTIA/Public Technology Institute reported that 69% of local governments are paying higher cyber insurance premiums. Cyber risk management tools can provide a strategic roadmap to assess the current environment, mitigate existing vulnerabilities, and prioritize future investments to provide an IT environment that delivers more trust and accountability.

**Create a reliable data backup and recovery platform**

Since 2020, there have been 3,200 known attacks against public sector entities and ransomware infections affecting five of the world's 50 largest information technology providers; nobody is immune from a potential attack. The common theme for organizations is "not if, but when." From a CyberEdge 2021 report – 69% of global organizations were compromised by ransomware and 57% of those ransomware victims paid ransom. In 2021, the average global cost to remediated a ransomware attach rose to $1.5 million, more than double the previous year's average of $761,106. A ransomware attack in early 2020 on the New Orleans city government cost the city approximately $7 million.

As part of an overall business continuity strategy, a reliable data backup solution is needed for various reasons including a ransomware attack. Most traditional data backup solutions are potentially compromised because of the unknown time and nature of the ransomware infiltration. In addition, these backups are usually housed on the same network infrastructure that has been compromised.

Combining hardware and software that provides a trusted and uncontaminated data backup in a separate set of servers (electronic vault), a secure system is isolated so it is available to restore critical operations in the event of a cyber-security event or other lock out of critical systems and data.

A cyber recovery backup solution enables rapid recovery of operations in the event of a ransomware attack. It creates a secure data backup that is protected and isolated from attack which allows for a quick recovery of critical data and systems. Using advanced zero-trust security features, this backup is protected from attack and can provide confidence in dealing with any cyber event. This is becoming even more important as the rate of ransomware attacks increase and cyber insurance coverage costs are increasing.

**Modernize identity and access management that supports citizen digital services and improves workforce access**

The demand by citizens for more modern and improved customer experiences are growing in our government services. 81% of U.S. adults now own smartphones and access many different digital channels via a website or mobile application. The Commonwealth is currently operating with a legacy identity and access management solution that limits the ability to quickly manage and adapt resources to manage user logins, self-service registrations and identity databases. The result for the citizen experience is usually multiple user credentials to access different application systems, all within the same public-sector agency.

Creating a single door to citizen services means the user experience must be seamless and secure. Modern, cloud-based, identity and access management systems are available that can improve the citizen, and employee, experience as well as provide additional security features. Multi-Factor Authentication (MFA) and single sign-on (SSO) are essential to protecting our citizens and our government process. The journey starts with Identity: identifying who the user is, identify what they require access to, and identify their location. This project would enhance the Commonwealth's overall

cybersecurity framework, reducing long-term management cost for the entire Commonwealth Enterprise, while also improving citizens' experiences.

## Coordination to promote success

In our experience across a multitude of states, we have seen the negative implications for IT security decisions made in a black hole with limited communication and feedback around plans or strategic priorities shared between centralized information officers and agency IT leaders. When it comes to the security of critical systems and data, an entity is only as strong as its weakest link. The Commonwealth's IT systems are, at various layers, connected, sharing data pools, common IT architecture and shared service vendors. Bad actors who gain access to one entity are often in a position to leverage that access across the entire network, enabling them to lock down information and systems, disable systems or steal valuable data.

The Commonwealth must continue to empower its CISO to act across agencies and entities, taking a whole-of-government approach to security. Equally important, the agencies must stay coordinated on their own needs and expectations to allow critical IT leaders the ability to produce strategies that incorporate the individual demands of unique entities within the government.

Attracting the best and brightest security experts has become a challenge for those in both the public and private sector. As such, the Commonwealth must recognize it may not have the internal resources to accomplish its strategic goals. Coordinating with federal entities such as CISA, the National Guard and FBI, along with private sector entities, provides the additional resources for the Commonwealth to implement its security goals and maximize the ability to establish a more secure environment.

## Conclusion

Unisys applauds this Committee's efforts to learn more about the cyber risks facing industry and the public sector. While it is important that all levels of government work with the private sector to provide resources and tools to protect critical infrastructure and sensitive data, it is equally urgent that government turn the risk mirror upon itself and understand its own vulnerabilities. The legislature and Administration must seek out increased coordination amongst state IT users, foster greater recognition of security risks for state agencies, holds government IT leaders accountable in establishing a security path forward, but also provides the resources necessary to implement such a strategy.

I would be remiss if I failed to mention that to achieve the greatest return, the legislature and Judiciary should ultimately work with the relevant Commonwealth IT leaders to include their systems under the same review and protection as those I have suggested for agencies. 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 security issues and to find new ways to allow the state to take advantage of security innovations that produce better results 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.