pennsylvania
OFFICE OF ADMINISTRATION

Testimony

House Commerce Committee

HB 1010

February 25, 2020

Office of Administration

John MacMillan

Commonwealth Chief Information Officer

Chairman Keller, Chairman Galloway, and members of the committee, I am John MacMillan, Chief Information Officer (CIO) for the commonwealth.

On behalf of Governor Tom Wolf and Office of Administration (OA) Secretary Michael Newsome, thank you for the opportunity to testify on HB 1010 which amends Act 94 of 2005, the Pennsylvania Breach of Personal Information Notification Act.

First, I'd like to share a little background about myself. I was appointed Deputy Secretary for Information Technology and CIO in March 2015. I have over 33 years of experience in the Information Technology (IT) industry. For almost 19 years, I worked for one of the world's leading IT companies. I have had the opportunity to assist customers in several states, including New York, New Jersey and Washington, with complex application development initiatives. In Pennsylvania and Ohio, I was involved in projects related to data center consolidation, operations, and standardization that achieved operational effectiveness and saved millions. I also had the chance to work in Texas and Georgia on data center outsourcing.

With me today is Erik Avakian. He is the Chief Information Security Officer, or CISO, for the commonwealth. Erik has served in this role since June 2010. He is responsible for the information security strategy, governance, technical standards, security policies, risk management, compliance, and cyber-incident response. Prior to his appointment, Erik served as Deputy CISO starting in 2007. Erik has assembled a vast array of security experience and expertise including security delivery, strategy and design, architecture, risk assessment, policy, compliance, incident response, and investigations. He has led numerous enterprise initiatives to further improve the commonwealth's security posture. Erik holds industry certifications including Certified Information Systems Security Professional (CISSP), Certified in Risk and Information Systems Control (CRISC), Certified Information Security Manager (CISM), Certified Information Security Auditor (CISA). He is an Executive Board member for the Multi-State Information Sharing and Analysis Center (MS-ISAC). Erik collaborates with members of the National Association of State Chief Information Officers (NASCIO) and the Pennsylvania State Fusion Center (PACIC).

Act 94 of 2005 – Pennsylvania Breach of Personal Information Notification Act

Act 94 of 2005, the Pennsylvania Breach of Personal Information Notification Act, 73 P.S. § 2301, *et seq.*, requires any entity, including a state agency, to

notify any Commonwealth resident if there is a breach of the security of the entity's system maintaining, storing or managing computerized data that includes personal information (PI). A breach is defined as the unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of PI maintained by the entity. PI includes the person's name in combination with or linked to their Social Security number, driver's license number, financial account number, credit card or debit card information.

This session, seven bills have been introduced to amend and update Act 94: HB 245, HB 662, HB 1010, HB 1181, SB 380, SB 487, and SB 955 (which is a companion bill to HB 1010). Since 2005, there have been many changes in technology, cybersecurity, data security, and data privacy. OA is very supportive of updating Act 94.

In prior sessions and in this current session, OA has worked with the General Assembly and the County Commissioners Association of Pennsylvania (CCAP) on the concepts and language to update Act 94. One of the most significant recommended changes to Act 94 is to expand the definition of PI to include: a passport number, a taxpayer identification number, a health insurance number, medical information, and biometric data. HB 1010 includes these items in its definition of "Personal information."

One of the changes OA would recommend is to change the definition of breach from "breach of the security system" to "breach of personal information." Security systems can be "breached" or "attacked" without the unauthorized release of information. What is important is taking the time to determine if a breach of personal information actually occurred **after** the discovery of a potential incident or attack on the system. I will discuss what I mean by "determination" in further detail below.

In addition, OA would recommend that a definition of "unauthorized" be added to the Act, in order to assure that use of data that has been authorized by certain federal laws, court orders, or with written permission of an individual is not subject to the notification required by the Act.

An important matter to consider is the time period for notification to the individual following discovery of a breach. HB 1010 maintains the current Act 94 notice requirements that notice be made "without unreasonable delay." We are supportive of retaining that requirement. However, it is imperative that a definition of "determination" be included in any legislation amending Act 94. Determination should be defined as: "The final verification, following an investigation, that a Breach of Personal Information has occurred." It is vital that IT professionals have the tools and time to

verify that unauthorized access to PI has actually occurred. The detailed incident response procedure (IRP), discussed later, is our established approach for doing so. We worked with CCAP on the specific wording of that definition and strongly urge that it be added to Act 94. Other bills amending Act 94 seek to provide a specific time for notification to the individual following discovery of a breach of the security system. If the General Assembly wants to include a time-period for notification, we recommend that the time-period for notification be within 30 days from the date of determination of the breach.

As IT has continued to evolve since the passage of the Act in 2005, so has the terminology utilized to describe data and those who collect and manage it. OA would recommend definitions be added to the Act with respect to those who collect, use, process, or store PI, as well as definitions describing the types of data that comprise PI. Finally, we believe it would be helpful to update certain notice requirements including the methods of notice or of substitute notice under the Act.

What the commonwealth is doing on Data Security

Nationally, Pennsylvania has become a recognized leader in information technology and cybersecurity. In the past several years, the commonwealth has received numerous national awards including:

Year	Organization	Description
2019	NASCIO	Winner, Enterprise IT Management Initiatives, IT and HR Shared Services
2019	NASCIO	Finalist, Government to Citizen, Child Support Enforcement System and JobGateway Integration Initiative
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

Year	Organization	Description
2018	NASCIO	Winner, State CIO Special Recognition, Center of Excellence for Electronic Grants
2018	NASCIO	Finalist, Government to Business, Environmental e-Permitting Platform
2018	Government Technology	Top 25 Doers, Dreamers and Drivers, John MacMillan
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, e-Inspection 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
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

Since cybersecurity matters 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 is of paramount concern and the 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. According to published reports, recent ransomware attacks in Atlanta and Baltimore cost those cities $17 million and $18 million, respectively, as well as taking many city services offline for weeks. Meanwhile, the costs of ransomware attacks against Luzerne County government and the Philadelphia Court System have yet to be disclosed. 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. Hackers now use advanced, persistent threats to penetrate and hide within a network which are designed to siphon off information over a long period of time. Keeping up with, and trying to stay ahead of, cybersecurity threats and risks is a marathon that never ends.

In 2017, OA began a major restructuring of IT in the commonwealth, including cybersecurity, to standardize and enhance service delivery over the long run. One of the major benefits of the IT 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 22.7 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.

- The number of attempted hacks on commonwealth systems
    - per day: 749 million
    - per week: 5.2 billion
    - per month: 22.7 billion
    - per year: 273 billion

Over the past 12 months, there were about 1.5 billion incoming email messages. Of those, 603 million email messages (40.2%) were blocked as spam or malicious by our email filtering service. Without the service, each of

the 85,000 end-users on our email platform would receive an extra 21 spam or potentially malicious messages every day.

Other key security services that OA provides to all agencies include end-user security awareness training, risk management services, policy compliance assessments, code reviews, and scans. For example, we perform vulnerability scans and 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, the service has been instrumental in limiting the risk of inadvertent data exposure.

During the fall of 2018, OA further formalized the commonwealth's response to potential security incidents by creating a detailed incident response procedure (IRP). The document outlines the respective roles and responsibilities of each organization in response to an IT security incident. The IRP covers all phases of an incident from discovery to triage to investigation to remediation and establishes the mobilization of the business, IT, communications, and legal teams needed to effectively respond to the incident. 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 Notification Act, HIPAA, or any other applicable law, we follow all requirements related to providing notification to affected individuals and, in some cases, notice to the public, as well. Conversely, if a security incident does not meet the legal criteria for a data breach, there is no requirement to notify individuals or the public.

A cybersecurity incident is a violation or imminent threat of violation of Computer security policies, acceptable use policies, or standard security practices. It's important to note that not all cybersecurity incidents are malicious attacks – accidents do happen. And not all cybersecurity incidents are what we would call a data breach. In fact, a data breach can only be called such following a determination from legal and business representatives, armed with the appropriate factual evidence that unencrypted or unprotected PI was accessed, acquired, or used improperly without authorization.

The IRP provides a standard process to respond to IT Security Incidents by all agencies, offices, bureaus, commissions, and boards under the jurisdiction of the Governor's Office.

The process provides a foundation for the timely and effective management of security incidents within the commonwealth, specifying procedures for identifying risks and legal obligations for investigating, responding, mitigating and recovering with respect to security incidents occurring within the commonwealth IT facilities as well as those hosted by service providers.

While the IRP standardizes a common process for all types of security incidents, not all incidents rise to the level of requiring forensics or log review. In fact, the vast majority of IT security incidents can be quickly remediated via automated processes and/or standard procedures. For instance, someone may click on a malicious email as part of a phishing scam. Our alerts are triggered, and we clean the impacted machine from the threat quickly without having to convene other teams and the impacted user can go about their business with no impact to data or downtime. In such a case, an incident is discovered, and then quickly remediated with recovery. For other less frequent incidents where there is a possibility that sensitive or personal data may have been accessed improperly, additional processes and analysis are required. This involves additional phases such as a thorough investigation with forensics and log review. In such cases, it's important that the legislation allows time for these vital components of the investigation to be completed so that the facts can be provided to the legal team and the business to allow for an accurate determination of whether there was unauthorized access to personally identifiable information. A thorough investigation involving log analysis and forensics is required and it cannot be accomplished without allowing the time for that to happen. OA has a standard set of tools and employees who are experienced in carrying out these tasks. Thus, this important available service capability is critical to obtaining an investigation which is accurate and defensible using industry standard tools and processes.

The IRP enables a fact-oriented approach that limits speculation and engages appropriate stakeholders during each of the incident phases. This involves multiple teams working in parallel throughout the incident process with the goal of improving incident response and associated communications during each phase. The Cybersecurity team (or CIRT) performs the technical analysis, log reviews and forensic investigation to determine the facts regarding what occurred, if data was accessed and what remediation is necessary. The IT Application/Support team works to restore system access for users to allow business functions to operate. The Business Team (or BIRT) handles business communications and coordination during each phase

of the incident with appropriate stakeholders such as press and internal leadership.

OA also collaborates on cybersecurity matters with the General Assembly through its IT leadership, Pennsylvania counties through partnership with CCAP, academia through our partnership with Harrisburg University and newly established partnerships with several cities and intermediate units (IUs).

OA provides the General Assembly IT leadership with enterprise "Cybersecurity Advisories" and awareness of existing cybersecurity solutions. OA has also engaged General Assembly 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 working with NASCIO, the Internet Security Alliance, and other state IT leaders to raise awareness about opportunities to harmonize Federal legislation to reduce the cost impact on Pennsylvania. For example, the Health Insurance Portability and Accountability Act (HIPAA) requires the encryption of data in transit and at rest. The cost to design, implement, operate and audit systems for information security purposes that address such regulations is measured in millions of dollars from Pennsylvania's budget when such laws and regulations are not aligned with each other.

I offer one final and very important consideration. We strongly support HB 2009, which establishes a state Cybersecurity Coordination Board. On December 17, 2019, this committee reported HB 2009, and it received First Consideration in the House. The Cybersecurity Coordination Board is modeled after the State Geospatial Coordinating Board (Act 178 of 2014). The State Geospatial Coordinating Board has been very active, valuable, and productive in addressing and coordinating geospatial matters across the state. The Cybersecurity Coordination Board would help coordinate data security matters across all levels of government in the Commonwealth and the private sector. We believe creating the Cybersecurity Coordination Board could be one of the most important and valuable -- short term and long term -- legislative actions that the General Assembly could take with respect to data security.

Again, on behalf of Governor Wolf, 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 testify before this committee.

*** END OF TESTIMONY ***