pennsylvania
OFFICE OF ADMINISTRATION

Testimony

Senate Communications and Technology Committee

Data Privacy

February 5, 2020

Office of Administration

John MacMillan

Commonwealth Chief Information Officer

Senator Phillips-Hill, Senator Kearney, 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 submit testimony regarding data privacy.

Data Privacy v. Data Security

Data privacy and data security are often used interchangeably, but they are not synonymous. They are two very distinct concepts, and there are major differences between the two.

Data security protects data from being accessed by bad actors such as external hackers or malicious insiders. This typically is known as cybersecurity or information security. The position within organizations that oversees data security typically is the chief information security officer or CISO. Erik Avakian is the CISO for the commonwealth and has served in this role since June 2010. OA works constantly to stay on top of the latest threats and respond to changing security needs.

Data security has existed as long as there has been data to secure, whether that means regulating which employees have keys to which filing cabinet or password-protecting certain databases. It is an area of growing significance for private companies and public entities.

Data privacy is a very complex area that is covered by privacy laws, regulations, and rules which govern how data is legally collected, stored, or used; how data is legally protected; and whether or how data is legally shared with third parties.

As the collection and use of data has grown, organizations are finding the need for a chief privacy officer to oversee data privacy matters. While chief information officers and chief information security officers most often have experience in the technology field, chief privacy officers usually are attorneys with experience in the types of laws that govern the protection and permissible sharing of information.

Examples of Data Privacy Laws with which the commonwealth Must Comply

There are numerous federal and state privacy laws with which the commonwealth must comply. The commonwealth ensures compliance with statutory and regulatory data privacy requirements. Properly protecting the privacy of citizens' data in compliance with these requirements is of paramount importance to the commonwealth.

For example, the Health Insurance Portability and Accountability Act (HIPAA) is one of the most prominent federal privacy laws. HIPAA provides data privacy and security provisions for safeguarding medical information, including the electronic transmission of data. Enacted in 1996 to safeguard the privacy of patient personal health information, in recent years HIPAA has emerged into greater prominence with the increase of data breaches caused by cyberattacks and ransomware attacks on health providers and health insurers.

Under the Internal Revenue Code, all tax information is confidential. IRS Publication 1075 imposes additional data security requirements on state government employees that have access to federal tax information. Last year, Pennsylvania passed Act 15 of 2019 which brought the state into compliance with IRS Publication 1075. IRS Publication 1075 requires fingerprinting of individuals with access to Federal Tax Information.

Act 94 of 2005, the Pennsylvania Breach of Personal Information Notification Act, requires any entity, including any state agency, to notify individuals in the event their 'personally identifying information' (PII) held by the entity is subject to a data breach. A breach is defined as the unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of PII maintained by the entity. PII includes the person's name, Social Security number, driver's license, financial account, credit card or debit card information.

This session, SB 380, SB 487, HB 1010, HB 1181 are bills that have been introduced to amend and update Act 94. There have been many changes in technology since 2005, and OA is supportive of the concept 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 on the concepts and language to update Act 94 and would be eager to discuss these efforts with interested members. One of the most significant recommended changes to Act 94 is to expand the definition of PII to include: a passport number, a taxpayer identification number, a health insurance number, medical information, and biometric data. In addition, another significant recommended change is to add a definition that “unauthorized” use of data would include the additional data privacy protection by ensuring the data is protected without the authority or permission by written consent of an individual, or authorization under State or Federal law, or court order. Another recommended change is to provide a specific time for notification to the individual once there has been a determination that a breach has occurred.

What the commonwealth is doing on Data Privacy

First and foremost, the commonwealth is responsible for ensuring compliance with all laws, regulations, rules, and policies with respect to data privacy. OA takes this responsibility seriously.

As mentioned earlier, data privacy now is a growing area of significance for private companies and public entities. Many organizations are establishing chief privacy officers to oversee data privacy matters. The Office of General Counsel is in the process of hiring an individual with specific expertise in data privacy. In addition, due to the sensitivity of the types of data they manage and maintain, some agencies (like the Department of Human Services) already have staff dedicated to data privacy.

OA also is in the process of hiring a chief data officer. The chief data officer will coordinate with the chief privacy officer on information security matters, but the roles and responsibilities will be distinctly separate and different. The role and responsibilities of the chief data officer will be an expert with extensive data policy, master data management, and data inventory experience, who will set and drive the enterprise direction and continuously improve data strategy. The chief data officer will lead enterprise-wide governance and utilization of information-as-an-asset through data modeling, data analysis, data quality, and data sharing. The chief data officer will lead, manage, and expand upon the established open data program within the commonwealth, while establishing a further data strategy for internal data management that drives data-driven decision making.

Data management exists along a spectrum, from the PA Open Data Portal, through typical data storage and maintenance, to the protection of highly sensitive personally identifying information governed by law. The chief data officer and chief privacy officer will work together in their complementary positions to ensure the proper treatment and governance across the spectrum of all commonwealth-maintained data.

We believe adding the chief privacy officer and chief data officer will be a significant step in allowing the commonwealth to remain a national leader on IT matters that affect our citizens, their data, and their privacy.

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
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
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

Year	Organization	Description
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
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 and privacy 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.

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 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 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, 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.

OA also collaborates on cybersecurity matters with the General Assembly through its IT leadership, Pennsylvania counties through 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 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.

I offer one final and very important consideration on data privacy and data security. We strongly support HB 2009 which establishes a state Cybersecurity Coordination Board. The Cybersecurity Coordination Board is modeled after the State Geospatial Coordinating Board (Act 178 of 2014) which Senator Gordner sponsored. 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 privacy and 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 submit testimony to this committee.

*** END OF TESTIMONY ***