Written Testimony

SB 696

(amends Breach of Personal Information Notification Act)

House State Government Committee

&

Senate Communications and Technology Committee

June 7, 2022

Office of Administration

John MacMillan

Commonwealth Chief Information Officer

Chairman Grove, Chairman Conklin, Chairwoman Phillips-Hill, and Chairman Kane, I am John MacMillan, Chief Information Officer (CIO) and Deputy Secretary for Information Technology.

On behalf of Office of Administration (OA) Secretary Michael Newsome, thank you for the opportunity to present written testimony on SB 696 which amends Act 94 of 2005, the Pennsylvania Breach of Personal Information Notification Act (the "Act").

I apologize for not being here in person to testify. I am currently attending the National Association of State Technology Directors regional conference in Philadelphia. As the host state of this preeminent technology conference, my commitment to this event was made months in advance of the announcement of this hearing. Nationally, Pennsylvania has become a recognized leader in Information Technology (IT) and cybersecurity. In the past several years, the Commonwealth has received numerous national awards which I have attached to my testimony.

In lieu of appearing today, I did offer the Committees my availability to testify on another date, as well as to meet with the Chairs to discuss SB 696. My offer to meet with the Chairs remains open. Throughout my tenure as State CIO, I have met many times with Members of the General Assembly to discuss IT matters and continue to have an open-door policy to do so.

In past sessions over the past seven years, OA and the County Commissioners Association of Pennsylvania (CCAP) have collaborated to engage in discussion with Members of the General Assembly about SB 696 and propose amendments to the Act. OA remains open to working with the Committees and the General Assembly to enhance the Act with amendments that OA and CCAP previously developed and proposed.

From OA's perspective, there is still one very significant change to the Act that needs to be made. A definition of "determination" must be included in any legislation amending the Act. 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 and acquisition to any Personally Identifiable Information (PII) has in fact occurred. We worked with CCAP on the specific wording of that definition and strongly urge that it be included in

the amendments to the Act. In addition, OA recommends two specific changes to terminology in the current draft of the bill that would require contractors to provide notice to OA upon the discovery of a possible breach. This trigger for action, if an entity suspects improper access into a system, allows OA to quickly assess and investigate the situation while offering assistance to contractors where appropriate early on. Attached to this testimony is a proposed amendment that would make this adjustment.

In addition, the Department of General Services (DGS) has estimated that changes required by the bill to current contracts will have a significant fiscal impact on state agencies. Also, according to DGS, future contract costs would be increased to comply with the requirements in the bill.

Cybersecurity matters have been, and will continue to be, a major area of concern at the state and national level. Cybersecurity and protecting our citizens' data is of paramount concern and the top priority for OA. The potential costs of a successful attack can be substantial. South Carolina incurred over $30 million in costs to recover from a data breach at its Department of Revenue. 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 in 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.

We look forward to continuing to work with the Committees on SB 696 to update the current Act. The goal of the legislation should be to ensure, in a non-partisan manner, that protections are in place for our citizens in the event any actual data breaches occur.

Again, on behalf 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 the Committees.

*** END OF TESTIMONY ***

Appendix – Information Technology and Cybersecurity Awards

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

Year	Organization	Description
2021	NASCIO	**Winner**, 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

Year	Organization	Description
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
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

Year	Organization	Description
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