CYBERSECURITY ASSOCIATION OF PENNSYLVANIA

Dear esteemed members of the State Government Subcommittee of Government Information Technology and Communication and the Senate Communications and Technology Committee.

On behalf of The Cybersecurity Association of Pennsylvania, I thank you for the opportunity to submit this testimony to you on behalf of our members and community.

Currently, Pennsylvania has the third oldest breach notification law on record, only Minnesota and Wisconsin are older[1]. The Breach of Personal Information Notification Act (P.L. 474, No 94) passed on December 22, 2005 and became law on June 19, 2006. To put that into perspective of modern technology, the first iPhone was released in 2007 and ransomware didn't become a common word until 2011.

Senate Bill 696 looks to update this critical piece of legislation that serves to protect the residents of this Commonwealth against modern data breaches.

It is the opinion of the Cybersecurity Association of Pennsylvania and its founder Scott R. Davis that as drafted SB 696 does not protect residents or ensure Pennsylvania citizens are alerted timely when a breach of their data occurs.

Today, data breaches are reported daily and the risk of a breach of personal information for citizens are greater than anytime before.

According to DigitalGuardian.com, in 2005 only 157 data breaches were reported in the US. Including 66.9 million records exposed.[2] In the Verizon Data Breach Investigations Report for the year 2021 Verizon confirmed 5,212 data breaches and over 1.1 billion records breached.[3]

With over 14 data breaches a day, we must change how we look at data breaches. Cyber criminals are piecing together data from multiple breaches along with public data from sources like social media and compiling profiles of citizens opening them up to ransom, extortion, or even identify theft.

Data extraction or the collection of different types of data from a variety of sources means that a cyber criminal no longer needs data that is combined with an individual's first name or first initial and last name.

Each data breach is a source of data, and viewing it in that way "Section 2 Personal Information" should be expanded to include State or Federal Issued ID's beyond Drivers License or PennDOT issued IDs, Insurance Policy Numbers, IRS Tax IDs, Passport IDs, Military IDs, Biometric Data, or other categorized databases (license plate recognition systems or contact tracing databases) of citizen data which may or

[11] https://www.perkinscoie.com/images/content/2/4/246420/Security-Breach-Notification-Law-Chart-Sept-2021.pdf
[2] https://digitalguardian.com/blog/history-data-breaches
[3] https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

may not be tied to a individuals name. In my experience many states are including many of these as types of personal information and the Commonwealth should follow suit.

Section 3 provides for the notification process and timelines for State Agencies, State Agency Contractors, State Agency under the Governor's jurisdiction, Counties, School Districts, and/or Municipalities.

Excluded from this list include higher education and businesses that engages in whole or in part in the business of colleting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information[4] concerning citizens of the Commonwealth.

Ensuring every entity that collects, maintains, or stores data is responsible and has a legal obligation to report breaches of data. It should be the right of any citizen of the Commonwealth to be alerted and made aware when a breach of any piece of their data is breached

Also lacking is any penalty for covering up a breach or simply claiming ignorance that a breach was unknown. Every ransomware attack is potentially a breach of data as files were accessed, yet most organizations including both state and private do not have the tools in place to identify what or if any data was actually breached.

State laws that are found to have a single notification point (i.e. Attorney General's Office) that breaches must be reported and in some states are cataloged online for transparency. These states are assisting the cyber security community and individuals from across the globe identify data that has been breached.

SB 696 continues the practice of multiple reporting parties including the Office of Attorney General, CISO or a Designee of a State Agency, or the Governor's office of Administration. Simplicity is key and transparency here should be a priority.

Section 5.1 outlines encryption requirements for state employees and state agency contractor employees. Whenever outlining technical requirements, we advise caution when crafting legislation as the terminology or technology oftentimes will advance faster than legislation can keep up. Section 5.1 is strong on Data in Transit but should probably be included in SB 482 or state policies, allowing SB 696 to focus on the discovery, reporting, and penalties associated with data breaches.

Again we thank the esteemed members of the committee's for the opportunity to provide this testimony regarding Pennsylvania's Breach Notification Law.

[4] Wording similar from Maine and Georgia's breach notification laws – Page 34 and 60 of https://www.perkinscoie.com/images/content/2/4/246420/Security-Breach-Notification-Law-Chart-Sept-2021.pdf