TESTIMONY ON HOUSE BILL 1010

Presented to the House Commerce Committee

By
Melissa Anese, Government Relations Associate
Michael Sage, Chief Information Officer

February 25, 2020

On behalf of the County Commissioners Association of Pennsylvania (CCAP), representing all 67 counties in the commonwealth, I write to share our comments on HB 1010, which would amend the Pennsylvania Breach of Personal Information Act.

Counties take seriously their responsibility to protect personal information and want to implement the best possible cybersecurity standards and assure affected individuals are notified in a timely manner in the event a breach still occurs. It is critical that any data breach legislation take into account any issues that are likely to complicate counties' ability to understand what constitutes a breach and when action must be taken, and outlines timeframes for response that could be impossible to meet depending on the situation.

House Bill 1010 seeks to require notification when there is a "breach of the security system". In terms of protecting personal information, this definition can be a bit vague. Security systems can be breached or attacked without the unauthorized release of information. It is critical to take time to determine if a breach of personal information actually occurred after the discovery of a potential incident or attack on the system. The addition of the term "discovery" of a breach, based on the final determination that a breach has occurred and there is reasonable causation of loss or injury, would provide a more consistent interpretation of when the specified time period for notification to affected individuals begins. This term is currently not included in Act 94 and the addition would add clarity for establishing when the clock begins on notification.

The specified timeframe for notification requirement is an important subject to focus on as well. House Bill 1010 maintains the current Act 94 notice requirements that notice be made "without unreasonable delay." We are supportive of retaining that requirement, but the addition of a definition for determination is vital to ensure IT professionals have the tools and time to verify that unauthorized access to personal information has actually occurred. We have been working with the Office of Administration on specific wording for that definition and ask that it be added to Act 94. In the extreme case that there is a possibility that sensitive or personal data may have been accessed improperly, additional processes and analysis are required, including thorough investigation with forensics and log review. In such cases, it's important that the law 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.

In addition, counties request an appropriate timeframe for notification, as it can sometimes take time to contain and mitigate the breach and identify individuals who may be affected for notification. In HB 1010, there is a requirement to make a public posting. While notification is important, public posting or notification to the media bring forward concerns of attracting unwanted attention from the threat actors while also creating an illusion of little to no security within system which can lead to public distrust. Other bills that would amend Act 94 seek to provide a specific time for notification to the individual following discovery of a breach of the security system. With consideration of the investigative nature of this process, we ask that any time-period for notification be within 45 days from the date of determination of the breach.

Additionally, the legislation offers an exception timeframe of three days related to law enforcement involvement. This shortened window would be extremely difficult to comply with given these investigations can take much longer. One recommendation would be to clarify that notification may be delayed until the law enforcement agency gives approval to notify.

There are other definitions that could be added or use clarity in the data breach law. Currently in HB 1010 there is no definition for "unauthorized" though it is used repeatedly throughout the legislation. The addition of this term would 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 requirement.

Going forward, CCAP also believes that provisions related to vendors should be consistent, first to assure the owner or licensee is also receiving timely notice of any breaches from its vendors, and to clarify the window for further action by the owner or licensee does not begin until after the vendor provides notice of the breach of personal information.

Due to the rise in cyber security incidents, CCAP, counties and state agencies are already working together closely to improve security definitions and implement vital cybersecurity initiatives, including quarterly meetings, an annual cybersecurity conference, a self-assessment security toolkit and other projects. Our partnership has also extended to federal partners as well. Counties take extensive care to remediate any incident that may occur. CCAP's collaboration with the Office of Administration enables counties to leverage cost-effective security awareness training and anti-phishing exercise capabilities that allow for additional education at a shared cost.

While these intergovernmental partnerships have proven invaluable in protecting cybersecurity, we also support HB 2009, which would establish a state Cybersecurity Coordination Board. The Cybersecurity Coordination Board would help coordinate data security matters across all levels of government in the Commonwealth and the private sector. The establishment of this board could be monumental in the future of data security.

Counties take seriously their responsibility to protect information and want to implement the best possible cybersecurity standards and appreciate the opportunity to have representation on the board. Counties value the close working relationship between the state and counties to ensure the county voice is heard in IT decisions and best practices can be shared.

Thank you for your consideration of our comments. Please contact us if you have questions or need additional information.