COMMONWEALTH OF PENNSYLVANIA
HOUSE OF REPRESENTATIVES

JOINT PUBLIC HEARING

HOUSE STATE GOVERNMENT
SUBCOMMITTEE ON GOVERNMENT INFORMATION
TECHNOLOGY AND COMMUNICATION

AND THE

SENATE COMMUNICATIONS AND
TECHNOLOGY COMMITTEE

HEARING ROOM 1
NORTH OFFICE BUILDING
STATE CAPITOL BUILDING
HARRISBURG, PENNSYLVANIA

SB 696

TUESDAY, JUNE 7, 2022
9:04 A.M.

BEFORE:
HONORABLE RUSS DIAMOND,
MAJORITY SUBCOMMITTEE CHAIRMAN
HONORABLE JOE WEBSTER,
MINORITY SUBCOMMITTEE CHAIRMAN
HONORABLE SETH GROVE,
MAJORITY CHAIRMAN
HONORABLE KRISTIN PHILLIPS-HILL,
MAJORITY CHAIRWOMAN
HONORABLE ERIC NELSON
HONORABLE BRETT MILLER
HONORABLE FRANK RYAN
HONORABLE BENJAMIN SANCHEZ
HONORABLE KRISTINE HOWARD

I N D E X

TESTIFIERS

* * *

SUBMITTED WRITTEN TESTIMONY

* * *

(See submitted written testimony and handouts online.)

REQUEST FOR PRODUCTION OF INFORMATION

* * *

PAGE LINE PAGE LINE PAGE LINE

(None.)

P R O C E E D I N G S

* * *

MAJORITY SUBCOMMITTEE CHAIRMAN DIAMOND: (Portion of audio missing) -- the Government Information Technology and Communication. That's a lot of words.

My name is Russ Diamond. I'm the Subcommittee Chair, and I want to thank Chairman Phillips-Hill of the Communication and Technology Committee for jointly hosting this hearing on SB 696, sponsored by Senator Dan Laughlin.

I would also like to express my thanks to all the members and testifiers today for attending the hearing. Please note that in addition to the three testifiers we have today, we also have received additional written testimony from John MacMillan, the Commonwealth's Chief Information Officer, the Office of Administration; as well as Brianna Petitti, Government Relations Associate at CCAP.

I look forward to hearing the dialogue on this important issue.

MAJORITY CHAIRWOMAN Phillips-Hill: Thank you, Representative Diamond.

If we could now, I'd like to start with

member introductions. If we could start with the other gentleman from Lebanon County.

REPRESENTATIVE RYAN: I'm Representative Frank Ryan, Lebanon County, 101st District.

Thank you.

REPRESENTATIVE MILLER: Brett Miller, 44th District, Lancaster County.

SENATOR DUSH: Cris Dush, Senate District 25, McKean, Potter, Tioga, Elk, Cameron, Clinton, and Jefferson Counties, and part of Clearfield.

MINORITY SUBCOMMITTEE CHAIRMAN WEBSTER: Good morning, everyone. I'm Joe Webster, and I represent House District 150 in Montgomery County.

Thank you.

MAJORITY CHAIRMAN GROVE: Seth Grove, 196th District, York County.

REPRESENTATIVE NELSON: Eric Nelson, 57th District, Westmoreland County.

MAJORITY SUBCOMMITTEE CHAIRMAN DIAMOND: And virtually, we have Representative Sanchez.

REPRESENTATIVE SANCHEZ: Good morning, everybody.

Ben Sanchez from Montgomery County.

MAJORITY SUBCOMMITTEE CHAIRMAN DIAMOND:

I'd also like to mention that Representative Webster is the Minority Subcommittee Chair.

Thank you for being with us.

MAJORITY CHAIRWOMAN Phillips-Hill: Thank you, members, for those introductions.

I would like to turn it over to Senator Dan Laughlin, prime sponsor of SB 696 to give a few words about his legislation.

Senator Laughlin.

SENATOR LAUGHLIN: Thank you, Chairwoman. Thank you, Chair Diamond.

I'll thank all the Senators and Representatives for being here, as well, so -- any way, good morning. I'd like to thank the House State Government Committee, Subcommittee on Government Information, Technology, and Communication, and also the Senate Communications and Technology Committee for holding a hearing on SB 696.

SB 696 updates the breach of personal information notification act to require state agencies victimized by a breach identifying personally identifiable information to report the incident to those affected within seven days. As we are now all well aware, information security

is an endless battle. Accomplished hackers are smart, and they are sophisticated when it comes to technology. They enjoy the challenge of matching wits with the technicians charged with providing IT security for government corporations and financial institutions.

And that certainly makes Pennsylvania state government a big target for them, something that was all too clear last year when Insight Global, an independent state contractor, acknowledged that they had mishandled sensitive information that exposed COVID-19 contact tracing data and the personal information of some 72,000 Pennsylvanians.

We have also had a data breach that has been impacting many of our unemployment compensation claimants, who had their bank account information changed within their accounts. This led to unemployment compensation claims being paid out to unknown criminals. And to date, the impact and timing of the data breach is still unknown.

It is understandable that any agency victimized by a data breach might be embarrassed and reluctant to publicly report the incident,

but it is certainly much more important to immediately inform the citizens about the theft of their personal information, so that they can take the steps to protect their own assets.

The Insight Global case and the unemployment compensation situation are prime examples of the need for the State to act quickly to protect its citizens when a data breach occurs. I am not suggesting that any of the state government's IT systems are vulnerable to cyber attack, but we all know that hackers are relentless in their attempts to steal personal and financial information.

And that's what makes the provisions of SB 696 so vitally important. We can only hope that the hard work of the State's IT professionals will be effective in protecting our systems, but we must be ready to immediately respond in the event of a breach. This bill has won overwhelming approval from the Senate, and I look forward to working with my colleagues in the House to get the measure to the Governor's desk.

So thank you for holding today's hearing on this important piece of legislation, and I look forward to hearing all the testimony being

presented today. And I'd like to add just one other thing. I realize that our state agencies try very hard -- and it's unfortunate that we even need to run a bill like this, but quite frankly, I it's -- I think it's needed more than ever.

So thank you -- thank you all for holding the hearing today.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Thank you, Senator Laughlin.

And I would now like to turn it over to our first testifier, Ken Hess. He is the Deputy Secretary of Procurement at the Department of General Services.

Mr. Hess.

DEPUTY SECRETARY HESS: Good morning, Senator.

Chairs Grove and Webster, thank you for inviting me. And my thanks to Senator Laughlin for caring enough about the Commonwealth citizens to put this bill forward. Usually when I come before you, I am joined at the hip by CIO MacMillan. And I do have his statement with me. I'll just read a couple of excerpts from that, if I may.

And I quote: In past sessions over the past seven years, OA and the County Commissioners Association of Pennsylvania, CCAP, have collaborated to engage in discussions with members of the General Assembly about SB 696 and proposed 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, quote, determination must be included as any -- in any legislation amending the Act. Determination should be defined as the, quote, 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 -- and at this point, I'm just going to stipulate PII and PHI as the same for all intents and purposes -- has in fact occurred.

We worked with CCAP on the specific

wording of that definition and strongly urged 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 state agency contractors and state agencies under the Governor's jurisdiction to provide notice to the chief information security officer of the State agency or OA respectively, upon the discovery of a possible breach.

This trigger for action, if an entity suspects improper access into a system, allows the effective State agency and OA to quickly assess and investigate the situation, while offering assistance to contractors and State agencies where appropriate early on. And I gather that, as part of his testimony, he provided a draft amendment that would make that adjustment.

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

the requirements of the bill. Blah, blah, blah.

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 that an actual data breach occurs.

Okay. And I -- I wholeheartedly agree with CIO MacMillan's statements. And we certainly agree -- and he supports the assessment that I'm about to share with you about the potential costs and other impacts that I believe are unintentional, perhaps, as a -- that go to the specific language that was used. So allow me to explain.

First of all, DGS recognizes the tremendous importance of protecting the personal information of the citizens of the Commonwealth. The Department agrees with the legislature that breaches of personal information are a concern and not to be taken lightly. However, the language in the current bill gives us pause when considering the scope and the intended time, cost, and resources that would be required by the most literal interpretation of the provisions.

We are confident that this hearing will provide a forum to mutually explore and to close the gap between the legislative intent and to protect personal -- to protect personal information and procurement policy -- wow, that's a mouthful -- that covers a myriad of contracts which contain no PII or PHI of any kind.

In summary, we believe the bill is unintentionally overly prescriptive and that it applies to all new and existing State contracts for both goods and services, many of which involve no PII, PHI and are irrelevant to the intent and purpose of the bill. The Department believes that SB 696 can be much more effective and efficient by designating a spend threshold and not encumber COPA administrators by including PCARD [phonetic] and other small purchases of goods and services in screening an amendment as required by the bill.

The Department is concerned with the cost of resources that will be required as written, given the requirements for all new and existing contracts. Based on our data, it's determined it would cost the Commonwealth approximately $84 million dollars to renegotiate the total number

of active contracts and purchase orders. Further, there is the possibility of suppliers seeking to terminate, rather than accept additional responsibilities.

Representative Ryan, as I recall, you have a military contracting background, and you are very sensitive and aware of all of the conditions that we put on our suppliers and many times what that does in terms of their pulling back, lack of participation, increased costs, longer time, et cetera.

The Department is already seeing significant resistance to higher and higher liability coverage driven by exceedingly rare but potentially catastrophic data loss. Insurers are unwilling to provide coverage to suppliers that seek astronomical or unlimited loss protection. Our supplier pools are receding, owing to such onerous conditions and limiting entry for developing providers.

Further, there's the financial impact it will have on agency budgets and on local governments, municipalities, school districts, universities, et cetera. There is also the matter of a significant duplication of effort.

Our standard -- and I underscore standard -- IT terms and conditions, which I have in my testimony as Attachment A, already stipulate comprehensive provisions for data protection, encryption, attestation of compliance, notification of breach, et cetera, at both the corporate and at the associate level.

And I cited a number of sections for you to actually see the language that is attendant to our IT contracts. Further, in Exhibit B, those are our standard -- I'm sorry Attachment B is our standard non-IT terms and conditions. And while not as specific as the IT terms and conditions, there are umbrella stipulations with regards to background check, confidentiality, sensitive information, HIPAA compliance, insurance and so on.

Given that these preexisting protections are already a part of the applicable contracts, we respectfully submit that resources needed could be put to better use. So our recommendations: at a minimum, the Department recommends that SB 696, in light of existing contract terms, not apply retroactively. Secondly, that it be limited in scope to service

only, not goods, not construction contracts, which can reasonably be identified as requiring access to -- excuse me --- PII or PHI data and include a threshold for contracts it does apply to.

For these reasons, the Department of General Services and the administration opposes the bill as it is currently written. But I want to underscore that we recognize the validity of the intent, and I believe, as John said earlier, that we can work together to bridge that gap and make this a very useful piece of legislation.

Finally, I would say, you know, I've read some of the testimony on folks that will follow me, and they indicate -- and I think rightly -- that the law can't keep up with technology. And I think that's a very valid point.

This administration has adapted and continues to update and refine an entire suite of security policies and the attendant contract terms and conditions. So just allow me to share with you -- I'm going way back here. And this is in your -- in my testimony.

These are the security policies that we currently have in place and attendant to our

terms and conditions. So there's IT, SEC-OOO, information security policy, Internet accessible proxy servers and services policies, enterprise security auditing and monitoring, enterprise web application firewall policy, Commonwealth of Pennsylvania electronic signature policy, minimum standards for IDs, passwords, and multifactor authentication, enterprise e-mail inscription [SIC] -- encryption policy, minimum contractor background check policy, virtual private network standards, enterprise policy and software standards for agency firewalls, data cleansing policy, COPA policy for credit card use for E-government, policy and provisions for protecting Commonwealth electronic data, security information and event management policy, IT security assessment and testing policy, security incident reporting policy, proper use and disclosure of personally identifiable information, physical security policy for IT resources, encryption standards -- and I'll come back to that one in a second -- enterprise data loss, compliance standards, enterprise firewall ruleset, Commonwealth data center privileged user policy, and Keystone login and identity proofing.

So as I say, a complete suite of requirements and what I believe are well thought out and up-to-date prescriptions for our contracts involving IT services.

So I said I would come back to the encryption standards. Because the bill specifically calls out encryption, I just want to give you an example of trying to keep up with technology. And so here's the IT technology policy for encryption, SCO 31 [phonetic]. I'm not even going to try to get into the, you know, the technical aspects of the various types of encryption and bits and number of times and things like that. But what interested me was that this was written originally in 2009, and listen to the number of revisions that have occurred to this that have been necessary to keep up with technology: 2014, 2015, 2016, 2017, 2018, 2020, 2021.

So again, imagine you having to prescribe legislation at that pace. It -- I think that we can reach an acceptable middle ground that provides you and the Commonwealth citizens with the assurances, you know, from an umbrella point of view, and then allows us to continue to adapt

and adopt best practices as is required to maintain that security.

Thank you.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Thank you, Deputy Secretary.

I appreciate those remarks. We received the 130-page testimony last night at 6:00 p.m., which we shared with all of our colleagues here and those online. And I'm sure that they will, you know, in the next couple of weeks have plenty of time as we work through the budget to take it all in and begin to digest it.

DEPUTY SECRETARY HESS: Great. Thank you.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: And it is interesting to note Pennsylvania is one of only two states that since 2009 hasn't updated its laws with regard to data privacy.

DEPUTY SECRETARY HESS: Yeah.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: So I think it's really a very timely conversation for us to be engaging in.

One of the things I wanted to talk to you about before we turn it over to colleagues for questions --

DEPUTY SECRETARY HESS: Sure.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: -- if I could, was the fiscal cost that your testimony today provided, which was contrary to what the agency provided to the Senate Appropriations Committee for its fiscal note. So in that fiscal note that we received, the Office of Administration had indicated that the provisions in the bill, for informational purposes, they anticipated that OA's operating budget in the fiscal year would be impacted by 9 -- approximately $9.6 million. Your testimony here today has greatly inflated that number.

Can you talk about how in less than a year you've come to those numbers?

DEPUTY SECRETARY HESS: Sure. I can't speak for John. I'll do my best to surmise or share with you what my analysis is.

I think that, you know, when the definition was added of contractor of all goods and services --

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Well, that definition was in the legislation when it passed out of the Senate. Because remember --

DEPUTY SECRETARY HESS: Right.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: -- we don't put fiscal notes onto the legislation until it --

DEPUTY SECRETARY: Right.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: -- gets through Appropriations and through the Senate, so yeah.

DEPUTY SECRETARY HESS: I understand. At any rate, I believe that the Office of Administration looked at this in an IT centric, you know, existing, what does this mean for our existing relationships, our existing contracts? I looked at it from the alternative point of view, which is this is all goods and services.

And so what it appears is that either the, you know, I'm not sure whether it's intended or not, but what the end result of the language that's in the bill is, is that we're being asked to go back and renegotiate contracts for rock salt to put in provisions of PII and encryption. And I don't know that there's any value, quite honestly, in so doing. But to comply with the exact language, that's what would be required.

And so that is where the big difference came in the -- in the estimates. I think it --

I believe that's easily resolved. And as stated in my testimony, you know, and with John, we are certainly willing to explore those gaps and to understand what the fullest, you know, the true intentions are and to see that the legislation mirrors that.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Well, I appreciate that explanation. I think it's rather disturbing that that information is not provided in a timely fashion to the Senate Appropriations Committee. Obviously, that is a conversation we're going to have to have in the future, but appreciate the testimony here today.

I'd like to turn it over to the Subcommittee Chairman, Representative Diamond, for any questions.

MAJORITY SUBCOMMITTEE CHAIRMAN DIAMOND: Sure.

Deputy Secretary Hess, your testimony seems to indicate that implementation of SB 696 for your agency would involve, among other things, a duplication of effort. And you provided us with several attachments relating to your standard IT terms and conditions.

Can you explain to us briefly three

things. A, what are the duties required by your agency under the current breach of Personal Information Notification Act?

B, have you ever had to put these duties into practice due to a breach? And if so, what did you learn from that experience?

And C, what kind of challenges do you face based on the current law? Are there changes you would like to see made to the law as a result? And if so, what are those changes?

DEPUTY SECRETARY HESS: That's a mouthful. Okay.

So our current IT terms and conditions and our standard terms and conditions do contain language that require notification and disclosure of breaches. And in fact, that is one thing that I think that we can -- that we can level set. So for example, in our IT terms and conditions, we say that we want notification within an hour of discovery. That, I believe, is really important and critical and also happens to agree with what CIO MacMillan emphasizes as the key priority, so that we can provide the resources at that time to analyze and understand the scope and the scale and, perhaps, the -- whether it was a negligent

or whether it was a harmful actor.

And of course, that takes two completely different paths. And as you're aware, the current language has law enforcement provisions in it. So those are our current duties. We have those protections in place on both IT and on IT contract terms and conditions.

Let's see, have we had to exercise mitigation efforts due to -- what is it called, beach with an r -- data loss? Yes. One of the -- we have in place a contingent contract for financial monitoring and correction of personal financial information and accounts if it is something that is required as a result of a Commonwealth loss. If it's caused by a contractor, of course we have indemnification built into our contract terms and conditions. And so it is incumbent upon the supplier to provide those mitigations.

What do we learn from these things? Well, I know what I learned. Senator Laughlin mentioned Insight Global, for example. And I'm not being the IT person. I'm looking at this strictly from a contracting point of view, so I can't -- I can't say about the technology things.

But what I learned is that, yes, indeed this is a continuous improvement opportunity that we can't stop every single potential infraction and that, you know, what do you do about somebody that makes a mistake, you know, that an employee of a contractor or a subcontractor simply makes a mistake, not of any ill intent. And so I think that we have to scale our approaches accordingly.

So that's what -- that's one thing that I would say that I've taken away from this. They're not all, you know, folks in Ethiopia or some place trying to break into our systems in the dead of night.

Challenges, I will -- of the current law -- I personally like the current law. I think that the notification aspect, I get it, right. I got my own credit cards and bank account information and health information, and I would certainly want to know within a reasonable amount of time whether that has been made public. So I -- I get that, and I agree with it. But what I like about the current law is it provides the true experts, you know, the flexibility to develop and to maintain policies that keep pace with the marketplace.

MAJORITY SUBCOMMITTEE CHAIRMAN DIAMOND: So I do want to recognize that Representative Howard has joined us virtually.

Back to my original question, maybe put in layman's terms for the folks watching, again, let's go back to this duplication of effort.

DEPUTY SECRETARY HESS: Sure.

MAJORITY SUBCOMMITTEE CHAIRMAN DIAMOND: So why would it be a duplication, rather than just an incorporation of, you know, the language of SB 696 into what you already do?

Why would it be duplication?

DEPUTY SECRETARY HESS: So there's over 10,000 contracts and purchase orders in the pool that we would have to address. Some of them have these provisions that I described to you already in them. The question is whether or not they rise to the level of protection that you are seeking.

If they don't, then we're going to have to open negotiations with those folks. And then there are those that don't have those terms and conditions in them, and we're going to have to talk to those folks about incorporating them.

And quite honestly, any time you pick up

the phone and call a supplier to say, I'm changing your responsibilities, what do you think his response is to me?

MAJORITY SUBCOMMITTEE CHAIRMAN DIAMOND: So prospectively speaking then, I mean, we are already broaching the topic of the legislative process may not be able to keep up with technology. So then equally, would you not then issue contracts based on that same premise that if technology changes and there's, you know -- is that already in the contracts you offer or is there an improvement you can do that way?

DEPUTY SECRETARY HESS: So like for example, there are NIST standards, National Institute of Standards and Technology that are called out in our, among many others that are called out. And so if NIST, for example, changes a practice or adds a new condition, our suppliers are bound to adopt those. Now, we're on the hook if there are -- if there are additional costs related to that, but they cannot say no.

MAJORITY SUBCOMMITTEE CHAIRMAN DIAMOND: Okay. And then just one final point. I mean, you had talked about, you know, what do you do when somebody makes just an honest mistake.

DEPUTY SECRETARY HESS: Yeah.

MAJORITY SUBCOMMITTEE CHAIRMAN DIAMOND: I would -- I would just emphasize that it doesn't matter if it's an intentional breach into a system or a mistake. For those 72,000 people, the harm was the same. It doesn't matter whether it was caused by a mistake or an intentional breach.

So Senator, other questions?

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Thank you, Representative Diamond.

I'd like to recognize Representative Nelson for questions.

REPRESENTATIVE NELSON: Thank you, Madam Chair.

And thank you for your testimony, Deputy Secretary. At least in my understanding of the prime driver for this bill is the absence of notification that has occurred for citizens that have experienced a breach. A struggle I have with the retroactive enforcement, it definitely is much more convenient from a contract perspective, but existing contracts where we have seen government intentionally not notify citizens, how would you recommend we approach

that gap?

I mean, legally, it's a shame that we have to pass a law to require government notify the citizens, but if we would eliminate that retroactive, we're talking millions of citizens that would potentially be impacted and would then get the green light not to be notified.

How would you suggest we bridge that gap?

DEPUTY SECRETARY HESS: I think that most -- I will put most --

REPRESENTATIVE NELSON: And I know you're a contract guy.

DEPUTY SECRETARY HESS: Yeah. Most of our contracts say that notifications should take place within a reasonable period of time. And I think that sort of harkens back to the original law, as well. And again, I -- you know, whenever you put a firm fixed number on something, it always seems like there are exceptions that you beat your head against the wall.

REPRESENTATIVE NELSON: Let's build on the standard. We'll use the example of unemployment --

DEPUTY SECRETARY HESS: Sure.

REPRESENTATIVE NELSON: -- that was used

earlier. Brand new system, $30 million, horrendous security controls, which resulted in the breach of thousands of citizens. And after multiple hearings, the Department of Labor and Industry still refused to notify those citizens. Bank accounts were changed. Information was hacked. A pretty substantial hack. But it was government who chose, not the contract itself, but the actual administration, chose not to notify citizens.

So I recognize that's one step outside of the contract language --

DEPUTY SECRETARY HESS: Yeah.

REPRESENTATIVE NELSON: But without a bill requiring that notification, how will people know that their medical information was taken or their bank accounts were even changed?

DEPUTY SECRETARY HESS: I got to say -- I will say two things. First of all, I am not qualified to answer that. I am a contract guy, you know, not -- unemployment insurance is not my beat. So I apologize, but that's just the simple truth.

I am aware, however, that L&I took steps, right, because I am the contract guy. I saw a

very quick move to secure an agreement with a firm called ID.me. ID.me deals with the simple, can I prove who I am on the other side of this phone. And again, I'm not the technology guy, but it seems as though, from where I'm sitting, supplemental efforts were taken to try to bolster the verification to be more proactive than reactive.

Now, maybe that's after the cow left the barn, but --

REPRESENTATIVE NELSON: Now, your testimony -- and it was a gracious step for the Department to provide, you know, a higher level of protection for citizens that would proactively provide, but the citizens were never notified and I realize we may differ there. One question about penalties.

You know, a testifier, you know, a little bit later today is, you know, talking about there's an absence for penalties for covering up a breach. What are your thoughts on strengthening that? I mean, credit to the COVID company. They did step up to the plate and say, hey, we had a breach. At that time, they could have looked the other way. Accountability for

intentional, you know, nondisclosure.

DEPUTY SECRETARY HESS: Right. Well, I'll say this much.

First of all, from my review of Insight Global, they did have the protections in place that, you know, I think you're right -- I think the supplier stepped up and did the honorable and right things under those circumstances, as far as I know, from being, you know, an outsider looking in.

I was very pleased to see that we had the protections in place in the contract if we would have had to force them to do that. But fortunately, it appears as though our screening process -- and that's a big part of this -- got us a partner that is responsive and responsible and did do the right things.

And on the backside is the insurance. Right. I think I mentioned in my testimony that insurance is a big part of this. And let's see here if I can lay my fingers on it really quickly. There are all sorts of insurance requirements attendant to IT contracts. And cyber security is one of them. I -- it will take me about five minutes to probably find it in this

100-page document, but you have it. And I think that is the other part.

What does concern us though is that seriously when we are asked to negotiate a contract with unlimited liability coverage, that is just a non-starter. We cannot get folks to compete for contracts with those kinds of -- those kinds of protections.

REPRESENTATIVE NELSON: Thank you.

Thank you, Mr. Chair.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Deputy Secretary, before I recognize the Chairman of the House State Government Committee, I need to make this point.

DEPUTY SECRETARY HESS: Yes, ma'am.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: And that is that the Insight Global situation took care of itself not because of that contract, but because the news media broke the story. That's what happened. I don't believe that anything would have been resolved had it not been for cracker jack reporters who put this on our plate. Timely notification to people means that they don't have to learn about their data being breached on the evening news.

So with that, I'd like to turn it over to the gentleman from York County, Representative Grove.

MAJORITY CHAIRMAN GROVE: Thank you very much.

With your discussion with Chairman Diamond, you had mentioned that like if a Federal law would change like NIST --

DEPUTY SECRETARY HESS: Yeah.

MAJORITY CHAIRMAN GROVE: -- it would be automatically updated. So within your contract, you have -- let me see a good section to pull up.

DEPUTY SECRETARY HESS: Welcome to my world.

MAJORITY CHAIRMAN GROVE: You have a section with -- here we go, information technology product policies general. The contractor shall comply with the IT standards and policies issued by the Governor's Office, Administration Office of Information and Technology, including accessibility standard sets, IT policy, accessibility -- contractors shall ensure that services and supplies procured under the contract apply with the applicable standards.

In the event that such standards change during the contract's permanence and the Commonwealth requests that contractors comply with the changes -- changed standard that any incremental costs incurred by the contractor comply with such changes shall be paid for pursuant to change order to the contract.

DEPUTY SECRETARY HESS: Correct.

MAJORITY CHAIRMAN GROVE: Now, that is a basically admin policy you put specific language with. Like on page 29 of your contract, it has workers' compensation insurance for all the contractors, employees, and those of the contractors engaged in performing services in accordance with the Workers' Compensation Act.

If we would go back and change the Workers' Compensation Act --

DEPUTY SECRETARY HESS: Right.

MAJORITY CHAIRMAN GROVE: -- would you have to go back and change these contracts or it's just applied?

DEPUTY SECRETARY HESS: We would have to look at the specific language in that clause. So I can't say that sitting here.

MAJORITY CHAIRMAN GROVE: Okay. Because

when I look at -- now, that's page 29.

On page 28, we do have a data breach or a loss section. And it says, a contractor shall comply with all applicable data protection, data security, data privacy, and data breach notification laws, including but not limited to the Breach of Personal Information Notification Act of December 22, 2005, P.L. 495, No. 94 as amended.

So that -- the law we're amending is applicable to that.

DEPUTY SECRETARY HESS: That's correct.

MAJORITY CHAIRMAN GROVE: So all your IT contracts, if we change the law, are automatically updated with that because you already have that in your IT contracts, correct?

DEPUTY SECRETARY HESS: Right. So then the phone would start ringing, possibly, depending on the language in the contract, saying hey, we just saw that the law was changed. Let's talk about amending the contract. And this is what additional costs or additional, you know, whether they'd be one-time, I have to now buy encryption software, or you know, that it's a run-rate type of increase based on a service that

they provide over and over continually.

MAJORITY CHAIRMAN GROVE: Right. But within your contract, you also have -- I will say the catch-all clauses.

DEPUTY SECRETARY HESS: Yeah.

MAJORITY CHAIRMAN GROVE: You have boilerplate, right?

DEPUTY SECRETARY HESS: Yeah.

MAJORITY CHAIRMAN GROVE: At any time you can cancel a contract --

DEPUTY SECRETARY HESS: Correct.

MAJORITY CHAIRMAN GROVE: -- correct?

You can say, all right, 30 day notice.

DEPUTY SECRETARY HESS: Sure.

MAJORITY CHAIRMAN GROVE: You don't like it, go pound sand, right?

DEPUTY SECRETARY HESS: Sure.

MAJORITY CHAIRMAN GROVE: Though you could come back and say to your contractors, we care more about protecting personal identification of our citizens because that's what we have.

DEPUTY SECRETARY HESS: Sure.

MAJORITY CHAIRMAN GROVE: I mean, could you imagine if someone got ahold of the

Department of Revenue's data, Social Security number, bank account number, names, whole nine yards. Probably if they file online, there's probably a password.

So now I have a password that you use. I have your name. I have your address, possibly your signatures. I have everything I need to destroy your life, and there's nothing you can do about it because if I sign up for a credit card, is this your signature, Mr. Grove? Well, I -- right? You have everything you need.

So I don't know why a company would want to ensure that people aren't protected or from a government with all that information we house. And that's just one agency, one agency, on top of a multitude of others. So I mean, you have boilerplate languages in here. I'm trying to pull it up here.

You know, termination, Commonwealth may terminate the contract or purchase order issued against the contract in whole or in part without cause, no cause. See you later, right?

DEPUTY SECRETARY HESS: Yes.

MAJORITY CHAIRMAN GROVE: So again, I don't -- going back to your fiscal note, I -- I'm

not buying $84 million. I'm not buying hiring over 100 attorneys. I'm not buying any of that stuff. I'm absolutely not.

You know, maybe you have an argument with salt. I will give you that, but with these IT contracts, I do not see the need for the administration, DGS, or OA hiring hundreds of people for compliance with something that's already built into your contract. So I'm -- just from my perspective, I'm not buying the fiscal note.

I just looked on the Budget Office, did you work with comptroller's office on that?

DEPUTY SECRETARY HESS: Not yet, no.

MAJORITY CHAIRMAN GROVE: Not yet. So Budget Office doesn't even have a fiscal note on this.

DEPUTY SECRETARY HESS: Right.

MAJORITY CHAIRMAN GROVE: And they have bills that are still on second consideration in the House, let alone this major, I think some landmark legislation by the good Senator, to try to protect us. And you know, citizens are tired of data breaches. They don't trust us. They don't trust giving out their information.

So we need to do everything we can to protect citizens from data breaches. This is a good trust mechanism to say we take this seriously. I just -- I find the fiscal note or the fiscal implications of your testimony highly inaccurate. I would suggest you work with your comptroller and get a better capture on that, particularly since most of your IT contracts already have this in. It's there. We know it's in there.

So that's all I have. Thank you.

DEPUTY SECRETARY HESS: If I may --

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Thank you, Chairman Grove.

DEPUTY SECRETARY HESS: -- one of the things about canceling contracts is you need to have somebody standing ready to take on that responsibility, right? And so I would not say especially in the case of complex IT or somebody that's dealing with all of the Department of Revenue's data that you would willy-nilly in 30 days cancel a contract because having somebody waiting in the wings and ready to pick up that awesome responsibility is not available on every street corner.

MAJORITY CHAIRMAN GROVE: Well, I know one thing. Having taken over as Chairman of this Committee, I meet with IT people all the time, contractors and vendors. For every vendor you have, there's 10 other vendors that can do the same job.

Even as Representative Nelson was bringing up our Labor and Industry issues with unemployment compensation, I met with a vendor who actually could probably do a better job than what IT has now on the front end of it. But Labor and Industry is not openly bidding the Labor and Industry IT security software. They did a closed bid under emergency procurement, which I think maybe Representative Ortitay might want to know about.

So I mean, we're tired of it. I'm just telling you, we're tired of it. Our citizens are tired of it. We need fixes. And I think the three-bill package that the Senate sent over to the House is a great fix. I know we have two in the State Government Committee, one is in --

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Judiciary.

MAJORITY CHAIRMAN GROVE: Judiciary. And

that's what we're hearing from the residents. We talk to them. We talk to citizens every day, whether we like it or not. It's part of the job, right. And they are tired of it. They want trust. They want that insurance that when they send their personal information -- Representative Diamond here just had a great conversation with the Department of State a few weeks ago on just the Department pulling personal information from other State agencies.

People don't like that either because they're trusting your agency. I didn't give my data to these other agencies to use for their own tools. So that's what we're dealing with out in the public, and that's what these bills are trying to get at and fix, and I think through a very good way.

Now, obviously, we're always willing to work with the Department, but I just -- I'm not buying $84 million with 300 new employees. I'm not buying that, particularly since Budget Office hasn't weighed in on that. And I'm not buying that it's going to take a big leg work to change a contract that already has a state law built into it.

So thank you.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Thank you, Chairman Grove.

Representative Webster.

MINORITY SUBCOMMITTEE CHAIRMAN WEBSTER: Thank you, Chairwoman.

And I'm hopefully not just changing the total scope of our discussion this morning. I want to make a couple of comments, some of which I may sound like Chairman Grove a little bit in terms of the expectations of how we find some level of excellence around our security within the Commonwealth and across all the agencies. Then also, thinking through all of the ramifications, I guess I'd start with pointing out -- and this is a little bit off the bill itself, but any organization with the scale and scope of the business operations of the Commonwealth of Pennsylvania would have a chief information security officer and a cyber operation center and you know.

So while I would agree with Chairman Grove on a lot of the internal things we have to do to be better at protecting our own data and interactions, I might disagree with the amount of

expense required to -- for us to catch up, you know, to 17 years of, you know, just in this one area of contracting and other things, but across our IT environment.

I'm curious, without taking this too much further, but I assume that whether it's DGS or maybe the State Department, we obviously are connected to every one of these contractors. We probably -- they bill online and we pay online and all those kinds of things. Does that take us in another direction in terms of the amount of high value, you know, information that we really have in our systems? And what happens next in that regard?

And hopefully, I'm not talking enough to, you know -- any one of those online transactions potentially creates a tunnel. And so now I'm teaching people where they should be looking, but if you can sort of address -- those are the scale and scope that you as, you know, the Deputy Secretary would actually have to envision to create security excellence across, you know, to modernize where we need to be.

DEPUTY SECRETARY HESS: Well, I'll speak to it as much as I can. Again, most of I think

what you're getting at is the actual technology, and I just provide the contracting to enable those to acquire those services. But I can say that we have -- again, in those -- in those terms and conditions that I've provided -- we have specific terms for, I think the acronym is PICA. It's credit card transactions, and that there are special security provisions attendant to suppliers that provide like debit cards for the Commonwealth.

The other that you mentioned, I believe, is typically referred to in the industry as hosted data. Right. So it's not data that's resident here in the Commonwealth on our servers, but is, you know, in the cloud, in some cloud application, things like that. And we do have specific terms and conditions again, dealing with the security of hosted data as opposed to access to data that is, you know, within our four walls.

MINORITY SUBCOMMITTEE CHAIRMAN WEBSTER: When you're talking about that part, does SB -- make sure I get it -- 696 -- I wanted to say 9 -- I get the sixes and nines upside down here.

Does that address some of the relationships that you would have with hosted,

you know, with cloud servers and technology companies?

DEPUTY SECRETARY HESS: I don't think it affects it, quite honestly. You know, the requirements for encryption in the bill, I believe, are general enough to provide for OA to select varying level -- different types of encryption and employing other defensive mechanisms like firewalls and end-point access and multifactor authentication and so on. That it allows us to select the right combination of techniques or tools or even software to protect the data at rest or in transit.

MINORITY SUBCOMMITTEE CHAIRMAN WEBSTER: Chairwoman, thank you.

I was really looking forward to the Cyber Security Association. I send my regrets, but I do have a voting meeting. I'm departing.

Thank you.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Thank you, Representative Webster.

We are recording this hearing, so you will be able to go back afterwards and watch their testimony. Thank you for participating here today.

Thank you very much.

Are there any other questions?

Representative Miller.

REPRESENTATIVE MILLER: Thank you, Madam Chair.

And thank you for your testimony, Deputy Secretary. You said in your testimony that you're basically okay with the change -- changing of the notification language in the bill. You also said, however, that you would rather keep the other, the original law because of its flexibility component. And then you talked about about $84 million projected costs.

My comment is, what is the cost to the Commonwealth for not fixing this, and the cost to the citizens for the breach of their information?

That's a rhetorical question, but my question to you is the -- relative to your recommendations, you referenced not retroactive, service only, and threshold limits. In your estimation, if some of those were taken into consideration, what would be the potential costs?

DEPUTY SECRETARY HESS: That's tough. I don't know. But I think it could be several orders of magnitude less. That's the best answer

I have for you, Representative Ryan.

I would -- we would need to know, you know, we would have to close that gap on, you know, the one hour, seven days discovery determination, et cetera. And once we had that, then we could narrow down that 10,000 to something else. And you know, if that something else is 100, 200, that's one thing. If it's, you know, we go from 10,000 to 9,900, that's something else.

And I can't answer that sitting here without us working together to get to that definition of notification and of discovery and determination.

REPRESENTATIVE Miller: So in your estimation from a contractual standpoint, I know you're not the IT person, but if we do nothing but change the notification system and keep everything else the same, will that provide significant and substantial amount of protection for the citizens from further breaches.

DEPUTY SECRETARY HESS: I'm not the IT guy. I'm sorry.

REPRESENTATIVE Miller: Okay.

DEPUTY SECRETARY HESS: I'm going to pass

to John on that on.

REPRESENTATIVE Miller: All right. Yep. Very good.

DEPUTY SECRETARY HESS: (Inaudible).

REPRESENTATIVE Miller: Thank you very much.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Thank you, Representative.

Senator Dush.

SENATOR DUSH: Thank you, Deputy Secretary.

I'm sorry. I had to step out and run four bills in my own Committee, and I'm back. I'm glad you're still here. Yes, I'm juggling like crazy.

In your testimony, you had -- you were stating that the -- we were talking about the breaches that Senator Laughlin had spoken of, but you said there were things in place already.

Would they have prevented or were there failures on the part of those contracts? In specific -- sorry, I'm trying to catch up here. In -- it was in reference to the contracts that were already in place and having to go back and renegotiate those.

What is to prevent those failures from reoccurring, similar to those other two data breaches if we don't go back and renegotiate those?

DEPUTY SECRETARY HESS: It's again, hard for me to say. As your contracting officer, I often do not -- I am not aware, sitting here, of the root causes of the losses of data. What I have to rely on are the agencies, the investigating -- I think the Inspector General was involved with the Insight Global, the Department of Health.

And they, I believe, have a responsibility to come back to me to say, you need to change your terms and conditions because protection was not afforded. That has not happened. And so from where I'm sitting, it appears as though whatever losses of data have occurred, they have not been because we don't have the protections, the contractual protections in place, but because, you know, negligent or, you know, honest mistakes have occurred, which resulted in the loss of data or making public data. And again, I -- I don't know that I can put anything into a contract to turn a human

being into a machine.

SENATOR DUSH: Well, that's not actually what I was getting at. I'm sorry.

DEPUTY SECRETARY HESS: Oh, okay.

SENATOR DUSH: What I'm talking about is the delay in notification.

DEPUTY SECRETARY HESS: Oh, okay.

SENATOR DUSH: If we have to go back and contractually renegotiate that so that there is a more expedited notification of the public, of the potential brief --

DEPUTY SECRETARY HESS: Right.

SENATOR DUSH: -- is there anything in the contract right now? Was there a violation of the contract or anything like that?

And if not, then there is definitely a need then for us to ensure that our current contractors are under obligation to make those types of notifications in a timely manner.

DEPUTY SECRETARY HESS: I think that --

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Senator, the testimony was provided here today. Chairman Grove read through the contracting provisions and believes that the language in the contract would require updates to be met. And so

we've debated this provision, and so I will just respectfully ask if we could move on.

SENATOR DUSH: Gratefully.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Thank you.

SENATOR DUSH: I'm grateful for the information.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Absolutely.

SENATOR DUSH: Thank you.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Thank you very much.

I want to thank you for being here today.

DEPUTY SECRETARY HESS: Thank you.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: One last question, and then a thought. Can you tell me exactly how many contracts we have with third-party vendors that directly impact personal health information or personal information?

DEPUTY SECRETARY HESS: I cannot.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: You don't know?

DEPUTY SECRETARY HESS: No.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: You are in charge of all of the contracts --

DEPUTY SECRETARY HESS: Sure.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: -- here in the Commonwealth as the Deputy Secretary in the Department of General Services. I'm going to use a line that my predecessor in this chamber used often. And he said, if you can't measure it, you can't manage it.

If the Department of General Services doesn't know how many contracts they have that directly impact the personally identifiable information of its citizens or the personal health information of its citizens, I would take it one step further. If you can't measure it, you can't manage it, and you can't secure it.

The gentleman who is the prime sponsor of this legislation, he builds homes. He's a general contractor. When he builds a home for you, he hires a carpenter, an electrician, a drywaller, right, a plumber.

If one of those third-party vendors or subcontractors that he uses, they don't do what they're supposed to do, the buck stops with him. And I have to tell you that in this Commonwealth, when a third-party vendor provides a breach of personal information or personal health

information of one of the citizens of this Commonwealth, the buck needs to stop with you.

So I appreciate you being here today. I am very sorry that the chief information officer was not here to provide testimony and answer the questions of these members. But again, the buck has to stop with us. It is our responsibility.

We compel the people of this Commonwealth to provide that information to us. They don't have a choice. They have to pay their taxes, right.

DEPUTY SECRETARY HESS: Sure.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: And that means that we have to hold ourselves to a much higher standard. The status quo isn't working. You just ask anybody who has had their information breached by Insight Global, had their data breached through the unemployment compensation system, had their data breached when the teacher information management system at the Department of Education was breached. You talk to them, they would say the status quo isn't working.

The people of this Commonwealth deserve better, and I thank you very much for your

testimony here today, Mr. Hess.

DEPUTY SECRETARY HESS: Thank you.

I look forward to working with the Committee further.

MAJORITY SUBCOMMITTEE CHAIRMAN DIAMOND: If I could just backtrack on one thing. Did you say we don't know what the root cause is of these breaches? Because we do know what the root cause of the Insight Global data breach was.

Some supervisor somewhere, contact tracing supervisor, thought it was a good idea to upload data to an open Google doc that anybody who had the address for that Google doc could find that. Are you telling me that there's nothing in your contracts that prohibits that sort of data going to an open source such as a Google doc, and that no one at Insight Global knew that that would not be a good idea?

DEPUTY SECRETARY HESS: Of course not. Confidentiality provisions in the contracts clearly require the contractor to take every possible precaution, training, background checks, et cetera, of their employees to prevent such things.

And again to my point earlier to Senator

Dush, this does not appear to be a systemic or mechanical or digital breach that occurred with Insight Global, but it was simply and regrettably, very regrettably, individuals not being aware of the ramifications of the tools that they choose to use.

MAJORITY SUBCOMMITTEE CHAIRMAN DIAMOND: All right. Well, thank you, Deputy Secretary.

DEPUTY SECRETARY HESS: Thank you.

MAJORITY SUBCOMMITTEE CHAIRMAN DIAMOND: Appreciate it.

DEPUTY SECRETARY HESS: Yep.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Our next testifier today is Andrew Kingman, of counsel, State Privacy and Security Coalition.

Thank you, Mr. Kingman.

MR. KINGMAN: Hi. Good morning, folks. Can you all hear me?

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Please -- please begin your remarks.

MR. KINGMAN: Thanks very much.

Good morning, Chair Phillips-Hill, Chair Grove, members of the Committee. I want to thank you for your time today in consideration. My name is Andrew Kingman. I represent the State

Privacy and Security Coalition, which is a coalition of over 30 companies and trade associations in any number of sectors.

I also am a compliance attorney who has worked on maybe 30 different security incidents responding specifically on the State notice requirements, pieces of those breaches. So I have some experience actually working through the compliance provisions, as well.

Want to thank the Senate for their work on this bill. Really appreciate it. And you know, our amendments, we've provided some testimony as well as both a list of suggested amendments and a red line to kind of show how that fits together. And happy to take any questions on it.

Many of our edits are simply clarifying edits that make the bill a little bit easier and more specific. There are two issues that I wanted to primarily address. The first is simply including private entities in the electronic notification provisions of this legislation.

This is the type of notification that we, you know, often get that says we have noticed suspicious account activity. Please go check and

change your password. Make sure that, you know, if this wasn't you, that you are, you know, able to go in and keep an eye on your personal information here. So simply including private entities in that notice -- the ability to notify consumers quickly about those types of -- that type of activity.

The second deals with the encryption standards. And just, our feeling is that having sort of Pennsylvania-specific promulgated encryption standards from the executive branch may not be the best fit given that many, you know, private entities and contractors work nationally, given the rapid evolution of encryption and how quickly technology changes, that allowing that technology and allowing entities to sort of use the latest and greatest encryption technology may be a better approach here.

So those are our -- those are our suggested edits. Happy to take any questions, but those are our -- that's the gist of where we're headed here.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Thank you very much.

Chairman Grove.

MAJORITY CHAIRMAN GROVE: Thank you so much for your testimony.

You were obviously here for the Deputy Secretary's testimony. We hear this a lot with when we try to do IT policy from the administration, that it completely takes away their flexibility. Putting in standards takes away their flexibility to manage. I'll tell you right now, many of us sitting here right now -- - not speaking for anybody -- but the General Assembly does not want to manage the executive branch's IT stuff at all. I have no interest in it.

But putting in guidelines, when you read SB 696, and having been someone who has dealt with IT in the private sector --

MR. KINGMAN: Sure.

MAJORITY CHAIRMAN GROVE: -- does this give -- take away any ability for any flexibility whatsoever to the administration to manage their IT?

MR. KINGMAN: Well, I think our concern is around just the pace of technology and the pace of policy, right. And so making sure that

if there are updates or improvements in encryption technology specifically, the businesses are not put in the position of, well, we're not permitted to use that because of guidelines that have been promulgated.

You know, I think that's the situation that we want to avoid, right, that entities are allowed to update their encryption methods --

MAJORITY CHAIRMAN GROVE: Right.

MR. KINGMAN: -- you know, as easily as possible.

MAJORITY CHAIRMAN GROVE: Right. And the underlying bill doesn't weight what encryption. It basically goes into if there's a breach, you must notify, correct?

MR. KINGMAN: That's right.

MAJORITY CHAIRMAN GROVE: Yeah. So we don't -- we don't stop the ability of the private sector to bring in new, I would say cyber security protections, or the administration to engage in increased cyber security protections. We're focused on this bill specifically as breached within the government arena, correct?

MR. KINGMAN: Sure. The provision that we were looking at was the section -- Section 4,

or excuse me, Section 5.1 with the general rule Subsection B. So Subsection A, we're advocating a change to allow not only encryption but other risk-based frameworks that would allow, again, as the Deputy Secretary mentioned, frameworks like NIST, the various NIST cyber security frameworks, ISO 27001 frameworks, the various frameworks that allow businesses to prioritize their vulnerabilities and put their resources towards the ones that are most effective to safeguard consumer data.

And then the next provision just making sure that those State contractors are allowed to use whatever the latest and greatest encryption technology is.

MAJORITY CHAIRMAN GROVE: Okay. And then the other issue you bring up -- and I guess we're doing this in a bit of a vacuum. You mentioned that a potential amendment in this bill would include private businesses and other entities. This bill is geared -- my understanding, it was a three-bill package. This bill was geared towards the government end.

MR. KINGMAN: Sure.

MAJORITY CHAIRMAN GROVE: That's why it's

in the State Government Committee.

MR. KINGMAN: Absolutely.

MAJORITY CHAIRMAN GROVE: There is another bill. I think Ron Mercuri has one, and you also passed one for the private sector. I believe is that Consumer Affairs again.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: So there is a ransomware bill, and that is also focused on government. The only piece of legislation, to my knowledge, currently in the General Assembly that addresses the private sector is Representative Mercuri's legislation that is in House Consumer Affairs currently.

MAJORITY CHAIRMAN GROVE: And I believe they're trying to work on that bill.

MR. KINGMAN: Sure.

MAJORITY CHAIRMAN GROVE: So I just want to let you know that is out there, and we --

MR. KINGMAN: No, and I appreciate that. Because this amends the underlying breach notification statute, we just want to allow businesses to also take advantage of that helpful notification process that tends to speed things up for that kind of suspicious account activity rather than go through a forensic investigation,

et cetera. So thank you.

MAJORITY CHAIRMAN GROVE: That's all I have. Thank you.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Thank you, Chairman Grove.

Interesting point that you make with regard to flexibility and assuring that government can use the most up-to-date security measures that they see fit to best safeguard the data.

So the challenge that we had with the updates to the unemployment compensation system was that the software actually came with multifactor authentication. A decision was made at the Department of Labor & Industry that it would be too burdensome to turn it on. And by not doing that, that was what created the opportunity for nefarious actors to get into people's personal bank accounts and their unemployment compensation account, change the banking information, reroute their money for unemployment compensation into their bank account.

So we want flexibility, right. We recognize that technology is constantly evolving,

that there are really smart people out there, every minute of every hour of every day creating new and better ways for us to secure sensitive information. But how can we assure that when we give the flexibility to those governmental entities that they will actually do the right thing and protect personal information with the best security measures?

MR. KINGMAN: Sure. And I think that's a fair question. Where our concern is more private sector-based, I don't think our role is to tell the State what -- how it should govern State agency contracts or anything like that. So our concern is more, you know, and specifically here just to encryption and just recognizing how quickly that technology has evolved. Making sure that businesses have a suite of tools available to them, not just encryption but, you know, again, any of the other, you know, firewall protection, end point security, employee training, things along that nature.

So we're more focused on the private sector implications.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Very good. Thank you.

Any other questions?

Representative Miller.

REPRESENTATIVE MILLER: Thank you, Mr. Kingman. Appreciate your testimony.

I have a question. Want to go back to Section 5.1 on encryption --

MR. KINGMAN: Sure.

REPRESENTATIVE MILLER: -- required. In that section, particularly Section B, you remove the statement related to transmission policy that the Governor's Office of Administration shall develop and maintain a policy to govern --

MR. KINGMAN: Sure.

REPRESENTATIVE MILLER: -- and so one. But in point A, the general rule is that State employees and State agency contractor employees shall, and then it goes on. But then you remove that from the Governor's Office.

Why would you remove from the Governor's Office the development of encryption and transmission policies but give it to State employees and State agency contractor employees?

MR. KINGMAN: The -- the rationale here on the amendments, again, was to -- so striking the from being viewed or modified by an

unauthorized third party, you know, our sense is that it should be to just protect the transmission of personal information over the Internet, whether that's from being viewed or authorized or other activities. You know, it should be protecting the information, not from what a third-party was doing.

And again, the other piece, it was not clear to us whether that was simply just State agencies or whether that would include contractors, as well. But again, the idea of just having the State set particular encryption standards, our concern is that the technology would outpace those standards, and that, again, businesses would be just put in the position of having to use, you know, outdated standards to safeguard their information.

That was the rationale there. We weren't trying to reallocate responsibility or anything along those lines.

REPRESENTATIVE MILLER: Okay. So is it -- is it your estimation that there could be a parallel or synchronous level of encryption technology knowledge in the real world and government policy working in a synchronous

fashion?

Or is there a setup that you can envision where the State policy and the current technology could be synchronous?

MR. KINGMAN: Well, I think an example would be, as the Deputy Secretary noted, you know, those -- those types of NIST frameworks or ISO frameworks that get updated regularly and sort of a built-in responsibility to continue evolving with those -- with those frameworks. That would be an example that, I think, gets at your question.

REPRESENTATIVE MILLER: Because I understand what you're saying, that policy does not keep pace with technology.

MR. KINGMAN: Right.

REPRESENTATIVE MILLER: But if there's a way that we can do that, I think that would be appropriate obviously. But I'm wondering in this language here, your suggestions, I have to study this more in depth because it almost seems like we give the responsibility to the contractor rather than the State policymaker. And I think that's exactly what we're trying to do, because as State policymakers, we have that as a

responsibility.

MR. KINGMAN: Right. Sure. I understand.

REPRESENTATIVE MILLER: I mean, I appreciate your attempt, and getting the technical language is tough. And we have to --

MR. KINGMAN: We would be happy to look at additional language if you had thoughts or --

REPRESENTATIVE MILLER: Okay.

MR. KINGMAN: -- anything like that.

REPRESENTATIVE MILLER: Very good. Thank you.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Thank you, Representative.

Mr. Kingman, thank you very much --

MR. KINGMAN: Thank you.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: -- for your testimony here today.

MR. KINGMAN: Sure.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: We very much appreciate it.

With that, I will welcome our final testifier today, Mr. Scott Davis, the President and CEO of the Cyber Security Association of Pennsylvania.

Thank you, Mr. Davis. And you can begin your testimony whenever you're ready.

MR. DAVIS: Thank you, Chairs, esteemed members of the State Government Subcommittee of Information Technology and Communication, and the Senate Communications and Technology Committee. Thank you for inviting me today.

On behalf of the Cyber Security Association of Pennsylvania, I thank you for that opportunity to submit the testimony on behalf of our members and the cyber security community in general. Also, thank you to Senator Laughlin for bringing this up and getting this bill present today.

Currently, Pennsylvania has the third oldest breach notification law on record. Only Minnesota and Wisconsin are older. The breach of Personal Information Notification Act, P L. 474 No. 94 passed on December 22, 2005 and become law June 19, 2006.

To put that in perspective of modern technology, the first iPhone was released in 2007. And ransomware didn't become a common word until 2011. It's fair to say a lot has changed. SB 696 looks to update this critical piece of

legislation that serves to protect the residents of the Commonwealth against these modern data breaches. It is the opinion of the Cyber Security 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 any time before. According to DigitalGuardian.com, in 2005, only 157 data breaches were reported in the United States. That included 66.9 million records of data exposed.

In the Verizon Data Breach Investigation Report for the year 2021, Verizon confirmed 5,212 data breaches and over 1.1 billion records breached. A lot of that is thanks to many states that have passed an updated breach notification law, forcing businesses to report and disclose breaches.

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, and identity theft. Data extraction, or the collection of different types of data from a variety of sources, means that cyber criminals no longer need data that is combined with an individual's first name or simply their first initial and last name.

SB 696 is a reactive bill. When I use the term a reactive in technology terminology, it means it's something that occurs after an incident has occurred. When you look at proactiveness, it's steps that are being done to prepare for something to happen. When we discuss a breach notification, it is always going to be a reactive because it is not triggered until a breach has occurred.

Every contractor, every employee, every agency has access to PII, to PHI, or records indicating a data breach. Each data breach is a source of data. And viewing it in this way, Section 2, personal information should be expanded to include State and Federal-issued IDs, beyond just a driver's license or PennDOT-issued

ID, insurance policy numbers, IRS tax IDs, passport IDs, military IDs, biometric data, or other categorized databases, such as license plate recognition systems or even the contract tracing database that has been talked about of citizens, which may or may not be tied to an individual's name.

Throughout multiple state government agencies, agency contractors, they have access to many of this data, yet this data is not protected with SB 696 as drafted. In my experience, many states are including many of these as types of personal information, and the Commonwealth should follow suit.

Section 3 provided for the notification process and timelines for State agencies, State agency contractors, State agencies under the Governor's jurisdiction, counties, school districts, and even municipalities. Excluded from this list includes higher education and businesses that engages in whole or in part of the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning citizens of the Commonwealth.

In a quick read of HB 2202, which was in the Consumer Affairs currently, that also is specifically targeting biometric data and does not cover PII as broad as this current SB 696 does. Ensuring every entity that collects, maintains, 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.

When I think of business technology, I work full-time for a cyber security firm out of Houston Texas called Liongard. Every one of our vendors goes through a stringent vendor questionnaire and security assessment before they are allowed to be a vendor. It should be no different for the Commonwealth of Pennsylvania to expect the same result from every vendor or agency that they contract with.

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 your files were accessed. Otherwise, they would never have been encrypted. Yet, most organizations, including

both state and private, do not have the tools in place to identify what or if any data was actually removed from that network, from that laptop, from that hard drive.

State laws that are found to have a single notification point, i.e. an Attorney General's office that breaches must be reported to timely, and in some states are cataloged online for full transparency. These states are assisting the cyber security community and individuals from across the globe to help identify data has been breached. Which is one of the reasons, like I stated earlier, Verizon being able to identify over 5,000 breaches over the last year.

SB 696 continues the practice of multiple reporting parties, including the office of attorney general, a CISO, or a designee of a State agency, the Governor's Office of Administration. Simplicity is oftentimes key. And transparency here should be a priority.

Section 5.1, which has been discussed previously, 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 technical requirements oftentimes will advance faster than legislation can keep up, which both witnesses testified to earlier.

Section 5.1 is strong on data in transit but should probably be included in SB 482, which is more geared towards the government's policies and rules set forth by legislature. Allowing SB 696 to focus on the discovery, reporting, and penalties associated with data breaches should be key, and leaving the technology aspects out of it. We agree with Mr. Hess that this bill should not legislate technology.

Again, we thank the esteemed members of the Committee for the opportunity to provide this testimony regarding Pennsylvania breach notification law.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Thank you very much, Mr. Davis.

Chairman Diamond.

MAJORITY SUBCOMMITTEE CHAIRMAN DIAMOND: Thank you.

Mr. Davis, I'm really curious about -- you talked about biometric data. And as I'm

thinking of this, as I hear biometric, I think of the movies where I, you know, somebody goes up and they scan the retina. And you know, they're given access to something. But as I'm sitting here thinking about it, am I correct in assuming that biometric data, as you are using it here, would actually be the merging of personally identifying information and personal health information?

Wouldn't the biometric data be touching on both of those things? Or am I not understanding what you're meaning by biometric data.

MR. DAVIS: I would say your health information is a piece of the puzzle. Your biometric data is a piece of the puzzle. When you look at combining databases, you're looking for points that are similar. It could be first name, last name, e-mail address, account name, et cetera, or Social Security number or beyond.

So if I was to gain access to the DMV database or on Real ID, I would gain retina images, I would gain facial impressions. If I was to gain access to a key card system that I use maybe to access a building or access a

security key or gain assess to an Android phone and be able to encrypt or decrypt access to the fingerprint, that is all biometric information.

There was a firm in the UK -- I apologize for not knowing the name off the top of my head -- that reported a data breach. It was one of the largest UK-based forensic or biometric data collectors for organizations, for businesses, for State agencies, that either used the retinas, either used the footprint -- thumbprint, but biometric data is still a person. It's a piece of the puzzle.

And if I'm able to now capture your signature, capture your account number, and capture a fingerprint or an iris scan, you're really opening up to beyond a current vision of a scope of a threat.

MAJORITY SUBCOMMITTEE CHAIRMAN DIAMOND: So does this -- does this fall on the same lines of things that we were talking about earlier, about not being able to keep up so that we have to -- if we would include biometric data in this law, is there a broad enough way that we could do that so that we're not limiting which technologies we're talking about?

MR. DAVIS: Absolutely. I think there's 14 or 15 states, if my memory serves me correct, that have biometric bills tied into legislation across the United States. There is a -- in my notes down below, number one, there's a URL that actually takes you through all of the breach notification laws across all 50 states, plus Puerto Rico.

MAJORITY SUBCOMMITTEE CHAIRMAN DIAMOND: All right. Thank you.

REPRESENTATIVE NELSON: Thank you, Mr. Chair.

I appreciate your testimony. I think you're raising some even larger concerns as, you know, you layer in those biometrics. At times, I think once somebody has your face ID, which the phones now use, or fingerprint, they really can go a lot further.

An earlier testifier, I asked them the question about, you know, consequences. When in your testimony you talked about lacking penalty for covering up a breach, what do you envision as an appropriate consequence for individuals or entities, because we could have both making those decisions?

MR. DAVIS: Most states, as I've read and understood them to read, put the penalty on the business. Oftentimes, mistakes happen due to lack of training. Proper training teaches you when not to click on e-mails or when to let your emotions run rampant and, you know, be opt for social engineering.

Social engineering is the act of designing an e-mail to get you to click to capture information. So oftentimes, the penalties are strictly focused on the entity that has allowed the breach to occur. It's typically a financial penalty through most of the legislations that I've read.

REPRESENTATIVE NELSON: And you mentioned also some states have a single notification point, so that businesses can go and everybody can kind of use that. Was that just appropriate action that government implemented on its own or was that achieved through a law that required such a portal to be listed?

MR. DAVIS: I believe in California's case, it was the law of CCPA, the California Consumer Protections Act, that passed several years ago and actually has been updated multiple

times since then. In many states, it is typically a law that is passed that is creating that database, if you will, that everyone that reports to.

REPRESENTATIVE NELSON: Okay. And my last question is, as we layer in the biometric data and pair that with an individual's personal passwords, once that information is out there, how does somebody readjust or resecure their retina scan or their face ID?

What happens following that breach in order to be able to correct somebody that will soon to be a victim if they're not already?

MR. DAVIS: Well, you can't change your iris. You can't change your face. You can't change your thumbprint. Well, I guess you could cut your fingers, but that's besides the point. You really can't change your biometric. It is who you are. And there is no methodology of erasing that data once it's been breached.

So once that data has been breached, really, I think today it's just sitting out there and waiting for the opportunity for when it is possible to utilize that to create a breach. Then that data will start to be used. There's

already tons of biometric data that has been breached that's out on the dark web.

REPRESENTATIVE NELSON: So in your opinion, do you feel this legislation should include elements that would incorporate protections for that biometric data or is that addressed in one of these other packages?

MR. DAVIS: This should be addressed in this bill.

REPRESENTATIVE NELSON: Okay. Thank you.

Thank you, Mr. Chair.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Representative Miller.

REPRESENTATIVE MILLER: Thank you, Mr. Davis.

Several questions. You talked about -- you're from Texas; is that correct?

MR. DAVIS: I'm from Pennsylvania. I work for a firm in Texas.

REPRESENTATIVE MILLER: Okay. Do you have familiarity with other states and their legislation in terms of a complete separation or siloing of personal information, say in our case PennDOT, keeping their information solely there, or Department of Health, et cetera?

Is there legislation out there in other states that keeps that information completely separate by statute.

MR. DAVIS: I am not aware. Part of my job duties at Liongard is to assist on security compliance questionnaires that we receive and understanding the 50 states and across the globe that we work with, including GDPR and essential aid for Australia.

REPRESENTATIVE MILLER: Okay. This -- my question was in reference to what was shared earlier about what's happening here in Pennsylvania. So we'll have to look at that. All right.

Do you have in your portfolio the gold standard of legislation somewhere in the states that is related to what we're doing? What states have the best in class out there related to what we're talking about here today?

MR. DAVIS: I truly believe California has set the pace and set the standard that many states are duplicating from.

REPRESENTATIVE MILLER: Okay. Question, you referenced in your business that you have an extensive questionnaire that you put all your

vendors through. Is that something you might be able to share with us or is that private material for your business?

MR. DAVIS: The one that is through my employer, I would have to validate, but I can provide samples.

REPRESENTATIVE MILLER: Okay.

MR. DAVIS: Or a simple Google search will provide many samples.

REPRESENTATIVE MILLER: All right. And the last question, the gentleman, Mr. Kingman before, provided some suggestions to the language that's in this current bill, SB 696.

Have you reviewed the bill?

You gave suggestions here in your testimony, but actual language, or could you perhaps do that to provide some suggestions for the Committee to look at?

MR. DAVIS: I can do that. I would just ask for some time as we are in the middle of a move, and I have three children.

REPRESENTATIVE MILLER: No problem. I'm not in the Senate. I don't want to speak for Senator Laughlin, but I think it might be helpful just to have multiple people providing input.

MR. DAVIS: Absolutely.

REPRESENTATIVE MILLER: Okay. Thank you.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: Are there any other questions?

Mr. Davis, I want to thank you. Your testimony was very helpful, and I think that there's certainly an opportunity to address, particularly, the concern about biometric data. Also appreciate your thoughts on ransomware legislation that is currently in the House Judiciary Committee.

I would like to thank all of the testifiers here today, all of the members who participated. Appreciate the prime sponsor of the legislation, his work to advance that legislation. And I do believe that it is in very good hands in the House with Chairman Grove and Chairman Diamond. Appreciate the opportunity to work collaboratively with them.

Any further remarks here today from either of the Chairmen?

MAJORITY SUBCOMMITTEE CHAIRMAN DIAMOND: I want to thank all of the testifiers as well as Senator Laughlin and the members for sitting in on this hearing today.

We have come a very, very long way. I remember my first -- my first foray into protecting people's data. And it must have been nearly three decades ago when I switched to electronic storage of people's credit card numbers at my business. It was very different than, you know, making sure that the carbon copy was destroyed. It was my first foray into that.

And I think this might be instructive, as well, is that my decision then was I would no longer score -- store people's credit card numbers, because I didn't want to be responsible for that information if someone broke into my office and electronically, you know, hacked into my computer or just opened up -- at that date, there were no passwords for computers back then either. So it would just be a matter of them smashing a window, opening a door, and going in and looking on my computer.

So I just opted not to store that data. And I'm wondering, too, if maybe the Commonwealth might be able to ask that question maybe a little bit more often, so that we don't even have this information circulating in Commonwealth cyber systems where it would be accessible. So we've

come a long way from, you know, carbon copies of credit card receipts to be destroyed to potential biometrics and theft of my actual face, retina, and finger print, but it is a great education.

And I appreciate everybody coming here today and the time we've spent on this.

MAJORITY CHAIRWOMAN PHILLIPS-HILL: And with that, I will now recess the Senate Communications and Technology Committee until the call of the Chair.

Thank you very much.

(Whereupon, the hearing concluded at 10:44 a.m.)

C E R T I F I C A T E

I hereby certify that the proceedings are contained fully and accurately in the notes taken by me on the within proceedings and that this is a correct transcript of the same.

Tiffany L. Mast

Tiffany L. Mast, Court Reporter

Commonwealth of Pennsylvania - Notary Seal
Tiffany L. Mast, Notary Public
Juniata County
My Commission Expires December 23, 2023
Commission Number 1237446