Joe Torsella, State Treasurer

Testimony of State Treasurer Joseph M. Torsella

House State Government Committee Hearing

House Bill 1704

November 14, 2017

Chairman Metcalfe, Chairman Bradford, and members of the committee, thank you for the opportunity to testify on cybersecurity today. I commend your focus on this important topic. Just last month we recognized National Cybersecurity Awareness Month, ironically amidst several major breaches of financial service-related firms that impacted many U.S. citizens.

Cybersecurity is a shared responsibility among every element of our state government that affects all citizens of the Commonwealth of Pennsylvania. As the primary financial institution of the Commonwealth, the Treasury Department is both a major target for cyber criminals and has a special obligation to secure the Commonwealth's financial information and payment processing responsibilities against cyber threats. We take this obligation and challenge very seriously, and work very closely with the Commonwealth's Cyber Security Officer, vendors and business partners to protect against cybersecurity risks, and to enhance information sharing on best practices.

While processing 20 million payments annually, Treasury interacts with all agencies and departments (77 in total) in the Commonwealth. Treasury is therefore not only concerned about its own security posture, we are vulnerable to the integrity of the data we receive from all our customers and business partners.

Cyber Threats and Trends:

Cyber threats represent a significant and growing risk to the Commonwealth and its citizens, threatening our security, economic well-being, and public health and safety. In the past 12-18 months, we have arrived at a tipping point where the breaches have reached truly extraordinary levels, affecting both public and private organizations. These attacks have affected multiple sectors of the economy, including, but not limited to, finance, health, defense, and politics. Institutions like the White House, NSA, various federal and state agencies, and companies like Yahoo, Equifax, and many more have suffered damage due to the actions of cyber criminals.

As a nation, we continue to experience threats from hackers, cyber criminals, and nation-states that are growing both more sophisticated and more frequent. We confront threats from both criminals seeking financial gains and nation-states seeking strategic advantage.

The most common threats are:

1. Phishing – An attempt to collect user credentials for malicious purposes through email, voice call (Vishing - Voice phishing), and text messages (Smishing). Phishing attacks usually involve sending authentic-seeming messages without personalized details to large numbers of people in the hope that one or more unwitting recipients will respond in some way that discloses valuable personal (or cyber) information to the attacker, allowing it to pursue malicious objectives. Recipients of phishing attacks may not believe that they know or have a relationship with the sender but fail to realize that the information they provide in response is sensitive or could be used by the original sender for malicious purposes.
2. Spear Phishing – A specific kind of phishing that involves targeted messages that contain personal information or details about the recipient intended to convince the recipient that they have a relationship with the sender and can provide sensitive information without concern. Spear phishing attacks frequently utilize data and information vacuumed from the recipient's social media postings and activities to deceive.
3. Ransomware – Taking user data and processes hostage to secure ransom.
4. Network penetration – Exploiting network vulnerabilities in order to get access to agency servers.

We can partly measure the growth of cyber threats by the amount spent on defending against them. According to a recent IDC report (International Data Corporation), $84 billion will be spent on cyber security products in 2017. That figure is expected to grow to $120 billion annually in the next four years. The financial industry alone has spent more than $16 billion annually to guard against cyber-attacks. A Gartner report finds that cybersecurity services is also one of the fastest growing areas of the economy. These numbers reflect the reality of the threats present in the world of cybersecurity, and the growing need for investment in protecting critical information infrastructure.

Treasury Cybersecurity Challenges:

Every one of Treasury's numerous business processes depends on our information technology infrastructure. Like any other agency in the Commonwealth, Treasury's IT infrastructure is complex and requires constant vigilance and upkeep. All of Treasury's PCs and servers need constant updates to their software to keep them current. Sometimes there are complex vulnerabilities in systems that have no obvious solutions. For example, the recently discovered vulnerability in Wi-Fi encryption standards has a universal impact with no quick resolution. These vulnerabilities are open to exploitation from unsavory actors.

Email is another area in which Treasury – along with many other organizations – experiences high vulnerability. Treasury receives more than **six million emails** every year. Only **15%** of these emails are

clean messages. **85%** of the emails are junk emails that often target innocent users with spam, malware, and phishing attempts. 75% of the emails are from disreputable sources.

Like most institutions with significant amounts of sensitive data and large IT capabilities, Treasury relies upon layers of security to increase our resistance to attacks. Treasury's firewall has in the recent past handled tens of millions of events annually. Due to the efforts of authorities like Europol and Interpol in taking down malware networks, and Treasury's multilayer defense approach, the number of events on our peripheral firewall has been reduced significantly. In spite of this progress, on average, four million events are identified and blocked as malicious events annually by Treasury's firewall. For obvious reasons we cannot discuss the details of Treasury's cyber defense efforts today, but Treasury's senior management takes cybersecurity extremely seriously, and prioritizes investments for IT security projects. But, as cybersecurity experts note, the weakest link when it comes to cybersecurity in any organization – including Treasury – is not any system but the people.

We believe an educated workforce is the best defense against cyber-attacks. Again, I should not disclose the details of our defensive program here, but we regularly circulate a cybersecurity newsletter, distribute special bulletins as circumstances warrant, and provide multiple classroom training opportunities every year. We recently implemented a program that requires every employee to take an online programmed learning course on current cybersecurity topics each month.

I should note that as Treasurer, even I am not exempt from this requirement, nor would I want to be: like every other Treasury employee, I was recently required to participate in these activities. In addition, we regularly invite experts from outside the department to educate our leadership team, so that we can learn the risks and integrate industry best practices in our own business processes.

Treasury completed a half dozen security projects this calendar year alone to further build up our multilayered defense approach, and we are working on a dozen more. At present, the responsibility of protecting our critical infrastructure is shared by many members of our IT infrastructure and application teams. With the General Assembly's assistance, Treasury anticipates transitioning to a dedicated and robust security team to provide for our security needs. We believe this approach will be much better suited to defending us from the evolving nature and growing sophistication of the cyber threats we will face. The team will support Treasury in the complex process of continuously keeping all Treasury IT systems updated and maintained at the latest patch levels.

Hence, Treasury is working towards a dedicated security team model. To that effect, Treasury is working with the budget office to establish an ongoing budget line item to fund cybersecurity projects and resources to staff the team, because cyber threats do not stand still. The threat changes and evolves, and so must our defenses.

Also, our internal audit team works closely with our IT team to provide oversight and monitoring of policies and procedures. This includes making sure those policies are updated to reflect current cybersecurity best practices and insuring that appropriate procedures are being followed. One challenge I should note here is that cybersecurity expertise is in great demand, the demand exceeds supply, and it is hard to recruit and retain cybersecurity professionals in the public sector.

Cybersecurity Oversight Committee:

In many organizations, cybersecurity is treated as simply an IT problem. I am glad to note that this committee is taking cyber threats as a serious strategic issue and pursuing proactive steps. I support and welcome the effort to establish a cybersecurity oversight committee, and I especially welcome your inclusion of Treasury in this effort. Although we are an independent agency, we must interact on a daily basis with virtually every other state agency. It is not an overstatement to say that our management of Commonwealth funds, investment activities and payment processing role provide existential support to these agencies. Each of us relies upon technology to operate, and our technology systems interact with each other multiple times every day. Our security concerns are therefore their security concerns, and vice versa. It makes good sense to encourage as much coordination and communication as possible.

Though every agency is at risk, not every agency shares the same risk profiles. I am confident this committee will create risk profiles for each entity and allocate resources accordingly. In addition, I would urge the Legislature to support all cybersecurity efforts across all agencies in the Commonwealth with the necessary resources to keep the Commonwealth's information assets secure and Commonwealth information processes functioning smoothly.

Conclusion:

As we face sophisticated threats, Pennsylvania Treasury stands on the front lines of the Commonwealth's efforts to defend our critical infrastructure from cyber threats. Our information technology infrastructure is complex and dynamic, with interdependencies that add to the challenge of securing and making it more resilient. As more and more processes depend on the computing power of machines, more attack vectors become available for our adversaries to take advantage of. As we pursue advanced technologies like cloud-computing, artificial intelligence, etc., we are increasing our footprint and access points. This is unavoidable, but we should recognize that it increases the probability of cyber criminals gaining unauthorized access to our information assets.

Most of the attacks are opportunistic, where perpetrators probe for a weakness in a system. These attacks can typically be prevented to a large extent by utilizing good business practices. Unfortunately, a sustained and determined attack from a nation-state that is determined to cause harm is much harder to prevent or defend against, for any organization. I know that the right people at Treasury – including me – go to sleep each night thinking about whether we are doing everything we can to protect our systems. I

also know that we are struggling to identify every weakness – including some that are unknown right now to anyone – and to anticipate every tactic or new tool about to be developed by smart and highly-motivated attackers. It is an incredibly high bar that we strive to maintain.

Such challenges cannot be managed by any single person, department or agency – it takes teamwork across bureaucratic lines, and making cybersecurity a priority across state government. For that reason, I again commend this committee's effort to think more broadly about this issue. As threats evolve, Treasury and the Commonwealth will also need to continue to modernize infrastructure to thwart any and all attacks, and to stay one step ahead of cyber criminals. We hope the Legislature will support and properly resource these efforts to ensure that Treasury and the Commonwealth can continue to maintain healthy cyber hygiene.

Thank you again for the invitation to testify before you today, and I look forward to your questions.