pennsylvania
OFFICE OF ADMINISTRATION

Testimony

Senate Communications and Technology Committee

and Senate State Government Committee

February 7, 2024

Neil R. Weaver

Secretary, Office of Administration

Chairwoman Pennycuick, Chairman Dillon, Chairman Dush, Chairwoman Cappelletti, and Members of the Senate Communications and Technology Committee and Senate State Government Committee, thank you for the opportunity to testify regarding the recent information technology limited data loss incident. I want to be clear: This was not a data breach, hack, or cybersecurity incident compromising any resident data. It was an incident of limited data loss, unfortunately caused by human error, that to date has been almost entirely restored or reconstructed.

I am Neil Weaver, Secretary of the Office of Administration (OA). As a member of Governor Josh Shapiro's senior staff and cabinet, I lead the agency responsible for human resources, information technology and other enterprise programs for nearly 80,000 employees under the Governor's jurisdiction. I have two decades of experience in non-profit and governmental management, operations, and communications. Prior to becoming the OA Secretary, I served as Acting Secretary for the Department of Community and Economic Development (DCED) and before that as Executive Deputy Secretary for DCED.

With me today is Amaya Capellán, Chief Information Officer (CIO) for the Commonwealth. Amaya became CIO in late July 2023. She has nearly 20 years of private sector experience in technology consulting, startups, and customer experience (CX). Amaya's last position was at Comcast, where she was instrumental as a leader of digital transformation for its customers. She helped launch Xfinity Mobile, Comcast's wireless service, and then led the strategy, pilot, and initial launch of Comcast Business Mobile, tailoring the service and offering for small, mid-size, and enterprise customers. Prior to joining Comcast, Amaya held product leadership and strategy positions at PeopleLinx (a venture-backed business-to-business sales startup), Booz & Company's Technology and Communications practice, FCB Global (an ad agency), and an eLearning startup in Madrid, Spain. In these roles, she helped to lead the companies through key moments of transition by working collaboratively to define products, strategies, and processes that leveraged technology to drive outcomes.

Also with me today is Jim Sipe. Jim started as the Chief Information Security Officer (CISO) for the Commonwealth in late November 2023. Jim is a seasoned cybersecurity leader, who has worked with some of the largest companies in the world. He has over 20 years of demonstrated experience working and advising across diverse industries. Prior to becoming CISO just 37 days before this incident occurred, he led an all-remote international team at Amazon Web Services that was responsible for IT security and technical guidance for the company's 25 largest global customers. Prior to his work at Amazon, Jim was an IT security executive for a digital communications and marketing company with over 29,000 customers worldwide, including Google, Facebook, and Uber. Jim also has extensive experience in cloud security and architecture, as well as disaster recovery and business continuity planning.

OA is responsible for the management and operation of IT services for all agencies under the Governor's jurisdiction. We also provide IT services and support to several independent boards and commissions. OA has an overall staff of approximately 2,400 employees. Of those, about 1,400 are in the Office for Information Technology. Their responsibilities include, but are not limited to:

- Managing nearly 133,000 end user devices like PCs, laptops, and smartphones.
- Hosting over 2,000 software applications supporting state agencies' programs and operations.
- Maintaining over 6,300 servers in our data centers used to host the applications I just mentioned.

- Responding to over 40,000 IT help desk calls and tickets per month.
- Blocking nearly 1 billion unauthorized attempts per day to connect to our network.

We have staff working 24 hours a day, 7 days a week, 365 days per year to manage, monitor, maintain, and protect the Commonwealth's IT resources. They are passionate about technology and public service and are motivated by the critical importance of ensuring these IT resources are working properly and available so that Commonwealth employees can best serve Pennsylvanians. As is standard across the IT industry in the private sector, many of our staff work remotely on a hybrid or full-time basis.

On January 3, an Office of Administration employee was performing routine server maintenance. Unfortunately, this employee made a human error that disrupted multiple agencies and resulted in the loss of data from two applications used by the Pennsylvania State Police (PSP) to manage and log evidence submissions, and from one application used by the State Employees' Retirement System (SERS) for members' online services account login. To be very clear again, this was not a data breach, hack, or cybersecurity incident compromising any resident data.

The same day, OA immediately notified all impacted agencies' staff of the issue and continued to provide regular updates. OA immediately began working to restore the impacted servers from backups. Working around the clock, the team was able to restore all but one of the 77 servers within several days. On Sunday, January 7, the team encountered difficulties restoring two applications for PSP and one application for SERS. OA notified both agencies that evening and began pursuing all potential pathways for partial to full recovery for all three applications.

As the OA team worked on restoration efforts, PSP and SERS alerted relevant members of the public – including law enforcement partners and customers – that the applications they used were unavailable and continued to keep them updated as applications were restored or rebuilt. Law enforcement agencies received instructions on January 12, 2024, on an alternative way to submit evidence or to inquire about case status. SERS posted updates on its website for members to regain access to their portal and reassured members that no retirement benefit data was lost, stolen, or inappropriately accessed. Additionally, OA, PSP, and SERS have provided several informational briefings to lawmakers since January 11 to keep them informed and answer questions.

The work to carefully reconstruct the remaining PSP data from various sources is ongoing. Data is being reconstructed through automated and manual processes by PSP lab personnel based on previous server data and images to ensure its accuracy and compliance with accreditation standards. I want to emphasize that all physical evidence tracked and cataloged by PSP remains secure and was never compromised.

Like you, we are incredibly motivated in understanding the who, what, when, where, why, and how so we can take the necessary steps to prevent anything like this from happening again. We have already taken several immediate steps to help mitigate this risk, and our review is ongoing. Additionally, we have engaged the services of a third party that specializes in helping organizations address occurrences such as this. This team has extensive experience in hands-on IT incident response, including assisting with the HealthCare.gov incident and ending California's unemployment claims backlog. They will assist us in our ongoing review and make recommendations to update our policies, processes, and controls – with the goal of ensuring nothing like this ever happens again.

As I mentioned previously, the work to reconstruct the limited PSP data loss is ongoing. Our review of the incident and recommendations are also ongoing.

Additionally, while I understand you and others still have questions about the incident, there are many aspects that we cannot discuss in public or for which we can only share limited details in order to protect the Commonwealth's cybersecurity.

As a reminder, we cannot discuss personnel matters. Questions have also been raised about whether working remotely contributed to this unfortunate incident. We can categorically affirm that it did not. As both Amaya and Jim can attest from their private sector backgrounds, remote work has been standard practice in the IT industry long before the pandemic and is essential to the Commonwealth's ability to compete with the private sector in the job market for IT talent.

Finally, in order to protect the Commonwealth's overall cybersecurity posture, there are many details about our IT operations and procedures that we cannot discuss publicly. For example, details about data backups, IT administrator access, and so on. Such information could provide insights to threat actors that, combined with other intelligence, could be used for malicious purposes. We thank you in advance for your understanding.

We appreciate the opportunity to testify and are grateful for all our partners who have worked diligently and collaboratively with OA on recovery and communication efforts. At this time, we will be happy to take your questions.

# # #