Statement of Lance Lyttle, Aviation Managing Director, Seattle-Tacoma International Airport

U.S. Senate Committee on Commerce, Science, and Transportation

"Aviation Cybersecurity Threats"

September 18, 2024

Chair Cantwell, Ranking Member Cruz, and members of the Committee, thank you for the opportunity to join you today. My name is Lance Lyttle, and I serve as the Aviation Managing Director for Seattle-Tacoma International Airport (SEA), which is owned and operated by the Port of Seattle.

The Port of Seattle is a special-purpose local government representing the residents of King County, Washington. In addition to SEA, the Port owns a major maritime gateway that includes international and domestic cargo operations, the largest cruise business on the West Coast, the homeporting of the North Pacific Fishing Fleet, and a variety of commercial and recreational boating marinas. SEA is the 11th busiest airport in the country by passenger volume, and the top ranked airport in the country three years in a row according to Skytrax.

We are here today because the Port recently experienced a cyberattack. While the incident has impacted our operations, we have made significant progress restoring services and systems. Importantly, at no point did this incident affect the ability to safely travel to or from Seattle-Tacoma International Airport or safely use the Port of Seattle's maritime facilities. Safety and security are our number one priority in response to this incident.

Alongside these restoration efforts, our own internal investigation is still ongoing. Our goal is to be transparent about this incident, but timing is critical. We are still investigating what data the threat actor obtained from our systems, and we are actively supporting the Federal Bureau of Investigation's (FBI) investigation of the incident. For these reasons, there is limited technical detail I can share at this time. We fully understand the importance of this information, and we are invested heavily in both understanding more about what happened and what lessons there are. To that end, we have engaged cybersecurity experts to conduct a forensic investigation, and we will be conducting an after-action review of this incident that will result in new information and insights.

In the interim, there are a number of lessons learned that we have already identified, which I am pleased to be able to share with you today. In particular, we are very proud of how Port employees and our partners came together to maintain continuity-of-operations throughout this incident, meaning that many of our passengers have had a relatively normal experience through the airport and our cruise terminals. I hope that my testimony today will help reassure air travelers of the safety, security, and resiliency of the aviation system.

Before I share some of those insights, I want to provide you with additional details about the incident. This incident was discovered when the Port of Seattle noticed unauthorized activity in our systems on August 24. It was a fast-moving situation, and Port staff worked to quickly isolate critical systems. However, both the attack itself and our responsive actions hindered some Port services, particularly at the airport – including access for some airlines to the baggage source messaging system, the check-in kiosks, common use ticketing, public Wi-Fi, airport display boards, the Port of Seattle website, the flySEA app, and reserved parking. Similarly, some of the systems on our cruise and marina side were impacted as well. Of note, the proprietary systems of our major airline and cruise partners were not affected, nor were the systems of our federal partners like the Federal Aviation Administration (FAA), Transportation Security Administration (TSA), and U.S. Customs and Border Protection (CBP).

Thankfully, we were able to keep most airport passengers on track by working with their airlines; by utilizing paper boarding passes and baggage tickets for the international carriers and lower volume carriers who rely on our common use system; and thanks to close coordination with TSA and CBP. I am very proud of the dedication, expertise, and resiliency of our employees, who demonstrated incredible knowledge of primary systems, backup systems, and manual systems. In addition, we are grateful to the Port employees from throughout our aviation and maritime divisions who contributed more than 4,000 hours over a ten-day period to help with operations, customer service, and wayfinding. For example, during the first days of the event, over 7,000 pieces of luggage were moved manually until some airlines regained the ability to access the baggage source messaging system.

Although there were some delays – particularly when a part of the baggage system was down – the airport has been able to successfully maintain regular operations. In addition, our team was able to bring the majority of the airport's operational systems back online within a week. Similarly, every cruise vessel left on time, and no travelers missed their sailings because of this incident.

Since August 24, Port staff have also been working with our technology partners and our forensics specialists to understand what happened, and we have been actively supporting law enforcement's investigation of the attack. As we shared publicly last week, we know that we were victims of a ransomware attack by the criminal organization known as Rhysida. While the efforts our team took to stop the attack appear to have been successful and there has been no new unauthorized activity since that day, our investigation has determined that the unauthorized threat actor was able to encrypt some of our computer systems and to copy some data from the environment.

As is typical in a ransomware attack, the threat actor sought to extort a ransom payment from the Port in exchange for providing a decryption key and deleting data they copied. On Monday, the threat actor posted the Port of Seattle's name on their leak site where they identify victims, as well as a copy of eight files stolen from Port systems. They plan to publish others in seven days unless we pay 100 bitcoin.

We are currently working to review the files published on the leak site as well as others we believe the actor copied. We will notify any individual whose personal information has been compromised, and will provide appropriate support. Fortunately, the Port has been able to validate that its backups were largely intact, and that no decryption key is necessary to restore our full operations.

The Port of Seattle has made the decision not to pay the perpetrators behind the cyberattack on our network. Paying ransomware to a criminal organization does not reflect Port values nor our commitment to be a good steward of public dollars. While we believe strongly this is the right approach, I can assure you that we take our employees' privacy very seriously, and this is not a decision that we take lightly. If we find that any employee's or individual's personal information has been compromised, we will notify them and provide appropriate support.

As I mentioned earlier, we are commissioning an independent after-action review and are continuing our own internal investigation. I look forward to being able to share additional details that we learn from our ongoing efforts. We also plan to share lessons learned with our peers throughout the aviation industry and others who operate critical infrastructure. And so, the insights that I am about to share are only preliminary.

In particular, I want to hit on three topics: 1) the effectiveness of cybersecurity systems, 2) the processes and practices that can ensure resiliency when faced with these issues, and 3) the Port's goal to be "stronger after" by incorporating these best practices into our future systems and plans.

We designed a robust IT and cybersecurity infrastructure to protect our systems from attack, and have received good feedback on both internal and external audits. Our staff is well-certified, experienced, and trained, and we have successfully detected attempts from some of the most advanced cyber attacks because of the strong program we had in place.

But there is no impenetrable cyberdefense, not only because cybercriminals are always evolving their tactics but also because an organization's protections are only as strong as the individuals who work within the system. Anyone who clicks on the wrong link, opens the wrong email, or connects to the wrong Wi-Fi is a risk – no matter how many annual trainings they are required to attend or multi-factor authentications (MFA) they are required to enter. We think that critical infrastructure and other organizations will face increasingly sophisticated cyber attacks. In our region alone, just in the last few months the Seattle Public Library and the Highline Public Schools were shut down because of cyberattacks.

Overall, airports take cybersecurity seriously, and have allocated significant resources to these efforts; major airport cybersecurity programs include a variety of policies, procedures and controls designed to identify and protect key assets, as well as respond to potential incidents. Examples include targeted messaging and training to raise cyber awareness throughout the airport; conducting penetration testing and vulnerability assessments; training and testing employees; and consulting with entities outside the aviation subsector to identify best practices and share lessons learned.

That said, there are definitely things we can do to further strengthen our security, and we regularly work to harden our cyber defenses. Our focus in the wake of this incident includes steps such as strengthening our identity management and authentication protocols, as well as enhancing our monitoring of our systems and network. For example, we have put greater protections around our active directory; made changes to keep our backup systems more secure and more quickly available; and added additional layers of restrictions so that major systems changes will have to go through additional layers of authorization.

Overall, we are learning the hard way about the pros and cons of separate systems versus vertical integration, the value and limitations of redundancies, and some of the technological workarounds that can quickly be put into place when main systems are offline. I want to thank our numerous external technology partners for their fantastic assistance during this incident – both to help us recover our systems and help us identify ways to build back better.

Second, in terms of resiliency, I am incredibly proud of our team for how they were able to spring into action and keep our airport operating, especially over the busy Labor Day travel period. The flights delays and cancellations in the initial few days of the incident were on par with a normal busy summer travel day. In fact, it is not an exaggeration to say that many travelers during this initial time period were unaware that we were having any problems at all, other than lack of access to public Wi-Fi and the fact that the Flight Information Display Systems (FIDS) and Baggage Information Display Systems (BIDS) were off.

Again, we benefitted greatly from incredible partnerships with airlines, federal agencies, and our tenants. In addition, from manually moving baggage to writing boarding passes by hand, we found ways to ensure continuity-of-operations. Again, thank you to the Port employees who spent hours in the terminal answering questions from travelers and manually accomplishing tasks that are usually automated.

As I said, we have learned many lessons from going through this experience. For example, I mentioned earlier that we developed workarounds – both on the technology side and process-wise – to keep people and baggage moving; many of those workarounds are quite effective and will absolutely go into our toolbox for future emergency response best practices. In addition, one of the key takeaways for us is about the importance of communications with all of our airport stakeholders – especially when our employees are locked out of the systems that they normally use for communications, such as email. There are tens of thousands of people who work at SEA on a daily basis – over and above the approximately 1,300 Port Aviation Division employees – and we need easily accessible ways to be able to update them regularly about what is working, what is still unavailable, and how to access information. During the first few weeks of this incident, we held daily teleconference calls, relied heavily on text message, used temporary signage, and did a lot of in-person communication. None of this is revolutionary, but when we have all become so reliant on technology it can be hard to readjust. For example, many airline ticketing agents and Transportation Security Officers had not seen or used a handwritten boarding pass, and so ensuring that this approach worked was a conversation with many parties.

On a related note, we have also established and strengthened a number of cybersecurity relationships that will be incredibly beneficial in the future. For example, some of our systems like the FIDS rely on airline data, and our airline partners wanted to be sure that our systems were truly secured before they re-connected; this discussion involved strengthening our high-level conversations with the cybersecurity leadership of their organizations. Similarly, we have received fantastic outreach from key federal agencies like the Cybersecurity and Infrastructure Security Agency (CISA); they have always been a great partner, but this incident has brought us closer together and opens the door to long-term collaboration opportunities such as better sharing of best practices and improving workforce development.

Finally, I want to talk about our goal to be “stronger after.“ Recovering from this incident has involved rebuilding some major Port systems from scratch, and it is not lost on me that we are doing work to restore and build systems that would normally take years to do, yet we are accomplishing things in a matter of weeks. Our technology partners have been fantastic at helping us build in better cybersecurity protections from the ground up as we do so.

It is essential that we learn as many lessons as possible from this challenging experience, and we are very hopeful that our continuing internal investigation and our third-party after-action review will help us identify additional best practices to improve our resiliency, our emergency preparedness, and our incident response.

Importantly, we do not want any other airport to have to go through what we are dealing with, and so we are dedicated to sharing best practices with peers throughout the aviation industry. We look forward to working with the Airports Council International, the American Association of Airport Executives, Airlines For America, CISA, the U.S. Department of Homeland Security, and many others to enhance the security of our collective operations. We have already begun conversations with TSA's Aviation Security Advisory Committee about how to utilize their forum, especially because TSA is the main regulator of airport cybersecurity. I want to be sure to call TSA out for being fantastic partners during this incident – both on the operational and the regulatory side.

I want to conclude by speaking briefly about ways that Congress and federal agencies can help the aviation industry be even more resilient in the face of these ongoing threats and challenges. In particular, government agencies should continue to proactively prioritize the dissemination of timely and actionable cyber threat information as soon as reasonably practicable; classified briefings should be provided at the earliest opportunity to highlight new and emerging threats.

In accordance with a TSA mandate, airports and airlines have been reporting cybersecurity incidents to CISA, and there are opportunities to improve the two-way sharing of information. The aviation industry benefits greatly from information about common cybersecurity incidents, and we need to make sure we are optimizing our security tools, talent, and properly resourcing our cyber ecosystems to focus mitigation efforts.

With that overview, I will end my remarks, and I welcome any questions you may have. Thank you again for your time, and for the invitation to be here today.