<u>Written Testimony</u>
Oregon’s Joint Committee On Information Management and Technology
Hearing on HB 2049

February 8, 2023 3:00pm

Chairs Woods and Nathanson and Members of Oregon’s Joint Committee on Information Management and Technology:

Thank you for inviting me to testify today on HB 2049. My name is Thomas MacLellan and I am the Director of Government Affairs and Strategy for Palo Alto Networks.

Palo Alto Networks is the world’s leading cybersecurity provider. Our mission is simple: “Be the cybersecurity partner of choice, protecting our digital way of life.” We have nearly 14,000 full-time employees located around the globe and protect many of the world’s most sensitive networks both here and abroad including: 10 of 10 of the Fortune 10; 8 of 10 largest U.S. Banks; 9 of 10 largest manufacturing companies in the world; 9 of 10 largest utilities in the world; 7 of 10 largest oil & gas companies in the World; and 9 of 10 top U.S. hospitals.

We have been recognized as a leader in Gartner Magic Quadrant Network for Firewalls; a leader in Forrester’s Zero Trust eXtended Ecosystem Platform Providers; a Leader in Gartner Magic Quadrant WAN Edge Infrastructure; a Leader in Forrester Endpoint Security Software As A Service Wave; a Leader in Forrester Zero Trust Network Access (ZTNA) New Wave; a leader in KuppingerCole Security Orchestration Automation & Response Leadership Compass; a Leader in Forrester Cloud Workload Security Wave; an Outperformer Leader in GigaOm's Attack Surface Management Radar; and we had the highest overall score in 2022 ATT@CK evaluations–100% prevention with least amount of configuration changes.

Innovation is key to Palo Alto Networks’ success. We began as a firewall company and have evolved to offer a full-service cybersecurity platform, and we continue to up our game in preparation for “what’s next.” Our ability to innovate and adapt is existential for us as a company—this is a must as threat actors become more sophisticated. This reflects one of the mantras in cybersecurity: as you modernize, so do the attackers.

The Cybersecurity Center of Excellence that HB 2049 would establish reflects the types of innovation that can help Oregon keep pace with these ever evolving threats. The areas on which HB 2049 focuses–workforce development, awareness and training, support of the unmet cybersecurity needs of regional and local government, special districts, Education Service Districts, K-12 school districts, and libraries–are at the core of the challenges facing states.

In my role at Palo Alto Networks, I have the opportunity to work across the entire nation and would like to share with you some thoughts and lessons that I believe will be of use to you moving forward. Given my limited time here today, I will focus on two areas included in the proposed legislation: workforce development and supporting the unmet cybersecurity needs of local governments.

Promoting a strong and diverse workforce. One of the biggest challenges facing the IT sector, and the cybersecurity sector in particular, is a shortage of qualified workers. For example, according to a recent study by ISC2[1], despite the fact that the global cybersecurity workforce has reached an all-time high of 4.7 million professionals, there is still a shortage of 3.4 million workers. In the US, this translates into more than 700,000 unfilled cybersecurity jobs.

Efforts to continue to grow and diversify the cybersecurity workforce are essential to meet this growing demand. This means starting in K-12 and continuing through to higher education and beyond. It also means diversifying the workforce by including more women and minorities.

At Palo Alto Networks, this belief is reflected in both our company’s core values of disruption, execution, collaboration, integrity, inclusion, and in our Corporate Responsibility program. For example, our Cybersecurity Academy Program, which we provide free of charge to educational institutions, helps prepare students for successful careers in cybersecurity. Currently, we are supporting over 1,850 Academy Programs in over 50 countries, including here in Oregon.

The Cybersecurity Academy offers a comprehensive set of courses covering cybersecurity fundamentals, cloud and network security, and operating a security operations center. These courses are aligned with the US National Initiative for Cybersecurity Education (NICE) framework for cybersecurity work roles and prepare students to be an integral part of the workforce of tomorrow.

In addition to the Academy Program, Palo Alto Networks funds fourteen $10,000 scholarships for students studying cybersecurity at Historically Black Colleges and Universities. These scholarships include mentorships with current Palo Alto Networks employees.

Palo Alto Networks also supports and sponsors cybersecurity “capture the flag events” that engage students at nearly all educational levels. These events have been very successful at attracting a range of new students from diverse backgrounds.

These and other similar types of opportunities are valuable in engaging a more diverse group of individuals to cybersecurity careers. Through the proposed Cybersecurity Center of Excellence, Oregon has the opportunity to scale similar efforts to make careers in these high-growth fields more attractive and attainable.

Supporting the unmet cybersecurity needs of regional and local governments. Given the interconnectedness and interdependencies of governmental networks and systems, more state and local governments are looking for opportunities to work across traditional boundaries in an

[1] ISC2 *Cybersecurity Workforce Study*, 2022, available at: https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

effort to provide more effective cybersecurity. This is driven in part by the shortage of qualified workers described above as well as economies of scale.

Of particular relevance here is the Department of Homeland (DHS) Security Cybersecurity & Infrastructure Security Agency's (CISA) State and Local Cybersecurity Grant Program (SLCGP). This program is the first-ever national effort specifically designed to strengthen state and local cybersecurity ecosystems by encouraging partnerships and coordination. One of the first and most significant decisions states must tackle is how to best leverage the grant to support local governments, especially as 80 percent of the funds must be passed through to them.

To leverage the collective power of the grant, state and local governments will need to adopt strategies that are scalable and support a larger unity of effort. There are effectively two ways to accomplish this: local governments banding together to support cross-boundary initiatives or states directly brokering services to local governments. In either case, the goal is adding net-new cybersecurity capabilities that close gaps and promote more secure government networks. These objectives align well with HB 2049.

Toward this end, there are a number of immediate actions state and local governments can take to greatly improve their cybersecurity posture.

1. **Support the adoption of real-time attack surface management capabilities.** There is a growing recognition that attack surface management is foundational to other cybersecurity controls and best practices. An "outside-in" view of your attack surface identifies assets and exposures organizations never knew existed. An entity that does not have an accurate, real-time understanding of what its internet-facing infrastructure looks like through the eyes of the adversary is working off an inherently incomplete and unstable cybersecurity baseline.

   Because manual asset inventory and point-in-time assessments are slow and prone to error, organizations need automated tools that can continually provide attack surface management monitoring. For example, Palo Alto Networks' Xpanse tool provides a complete, accurate and *continuously* updated inventory of all global internet-facing assets for organizations, including those in on-premise data centers and public cloud providers. Xpanse allows organizations to discover, evaluate and mitigate cyber attack surface risks in near real-time.

   It's worth noting that the U.S. Department of Defense recently adopted Xpanse to automatically identify its known and unknown internet-facing assets, prioritize them for remediation, and deploy playbooks to address critical vulnerabilities. States and local governments should have similar capabilities.

2. **Have incident response retainers in place prior to an attack.** By definition, disasters are unpredictable but that does not mean that governments can't prepare for the

unexpected. One way that state and local governments can arm themselves prior to an attack is to have incident response retainers in place so that when an attack occurs they are able to reach out for help at a moment's notice.

By way of example, last fall a local government's IT system was severely crippled by a ransomware attack that had far reaching impacts across the majority of governmental services. Unfortunately, they did not have an adequate incident response plan in place, including an incident response retainer by a qualified provider, and as a result lost significant time early in the attack which allowed the attackers to further penetrate into their IT infrastructure.

Pre-establishing incident response retainers to support state and local governments, can reduce latency in responding to an attack and help ensure that organizations can get back online as soon as possible.

3. **Support comprehensive risk assessments.** Another way governments can work together is to support risk assessment programs that help organizations understand how they rate across key domains including ransomware readiness, lifecycle security reviews and best practice assessments. Each of these are essential to helping organizations understand their individual exposure to risk.

   For example, Palo Alto Networks' Unit 42 works with organizations to assess conformance with best practices and standards, such as NIST, and also to assess how prepared they are for a ransomware attack. These types of assessments can include pen and paper assessments, table top exercises and comparison of how an organization's current security stack identifies incoming threats.

4. **Establish an automated joint security operations center.** Joint security operation centers (JSOCs) are an effective way for governments to band together to share information and respond to attacks. They provide a central way to understand specific threat vectors and scale a response. Additionally, because attackers often reuse tactics, techniques, and procedures (TTPs) that have been successful in the past, JSOCs can help similarly configured governmental organizations proactively remediate weaknesses. Finally, by leveraging effective automation tools, JSOCs can help address critical staffing gaps that may impact readiness and response capabilities.

5. **Secure the remote workforce.** Perhaps one of the biggest changes the pandemic brought was the blurring of traditional work boundaries. What was once termed "remote" or "hybrid" is now just "work." Today's workforce demands immediate, uninterrupted access for users, no matter where they are located. Unfortunately, existing network approaches and technologies do not provide the levels of security and access control organizations need. Organizations that adopt a new security concept known as secure access service edge (or SASE) are enabling a scalable approach that can support a remote workforce with a high level of security.

Working remotely requires a different security solution set, especially as data moves back and forth between the public cloud and an organization's internal network. This is why a Zero Trust approach to cybersecurity is so critical. Zero Trust is a cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted. It assumes that a breach has already occurred or will occur and therefore, a user should not be granted access to sensitive information by a single verification. Instead, each user, device, application and transaction must be continually verified to be able to access an organization's sensitive computing resources. This is especially important in a remote work environment where network boundaries have all but disappeared.

6. **Optimize existing technologies.** Many governmental organizations do not fully leverage the extant power of their cybersecurity capabilities. At the outset, many government security stacks are comprised of multiple point solutions that lack interoperability and do not allow for a true zero trust architecture. Effective security orchestration tools can help alleviate that weakness in the short term, but long-term solutions should look toward implementing more platform-based capabilities moving forward. A collateral benefit of such an approach would give governments the opportunity to add or turn on additional capabilities, through measures like subscriptions on existing next generation firewalls that will immediately add net-new capabilities at marginal costs.

In closing, I would like to offer to the members of the Committee an opportunity to receive a high-level threat briefing to help you better understand the current threat landscape and what it means to you as policymakers. I will follow-up with Committee Staff regarding this offer.

Thank you again for the opportunity to testify before you today. I look forward to your questions.