Testimony for the Record
Support HB 2049 (100000000001b)
Ray Blair
Distinguished Architect
Cisco Systems
Before the Oregon State Legislature
Joint Legislative Committee on Information Management and Technology
February 8, 2023

Good morning, Chairs Woods and Nathanson and members of the committee – I appreciate the opportunity to share Cisco's perspective on cybersecurity education and coordination.

My name is Ray Blair. I am a Distinguished Architect with Cisco Systems. My technology career spans nearly 35 years, and I am a proud Salem-area resident. I have three Cisco Certified Internetwork Expert (CCIE) certifications, including one in security. I'm a Certified Information Systems Security Professional (CISSP) and a Certified Business Architect. And I have coauthored four Pearson Education books on technology, one of which is centered around security.

Cisco is the worldwide leader in networking technology that provides the backbone of the internet, with 85% of the world's web traffic traveling securely across Cisco connections. Since our founding in 1984, Cisco has grown to become a market share leader in 11 technology segments including networking, zero-trust security, collaboration, and the cloud. Cisco's customers are governments, hospitals, schools – in Oregon and much of the world – as well as the private sector, including 98% of the Fortune 500.

Cisco's role in connecting and securing networks provides a unique vantage point of the constantly evolving cyber threat landscape, and strengthening security and resiliency will require increased public-private cooperation.

That is why Cisco is proud to support House Bill 2049 and its goal to create the Oregon Cybersecurity Center of Excellence (CCoE). The creation and support of the Center is a strategically important use of Oregon's resources. Increasingly, the work of government relies upon technology to ensure that public services are delivered efficiently, effectively, and securely. While we welcome the opportunity to partner with all government entities to help them meet their technology goals, we know not all organizations have the resources – time, staff, and funding – to accomplish everything alone. The CCoE is an example of one way for resource-constrained teams to learn from those who are further along in their digitization journey. Navigating the ever-changing cyber environment is a team sport. Bad actors are sharing information to improve their offense. State and local governments must do the same to improve their defense.

Threats and Collaboration

We are aware of the growing threats from malicious cyber actors. Today, these actors are well organized, highly funded strategic cyber organizations that present Advanced Persistent Threats (APT). We have seen attacks in the United States on critical infrastructure and state and local governments – from cyber intrusions at water treatment plants to ransomware attacks on hospitals and schools. These types of events upend everyday life and can have severe implications, ranging from service disruptions to even injuries or fatalities.

Cisco Talos is one of the largest commercial threat intelligence teams in the world – blocking 20 billion threats daily and comprising world-class researchers, analysts, and engineers. In 2022, Talos observed

several state-sponsored, offensive cyber campaigns linked to groups stemming from Russia, Iran, and North Korea, among others. These groups engaged in a variety of malicious activities, including espionage, intellectual property theft, and deploying destructive malware.

To combat cybersecurity threats, it is important that both the public and private sectors are empowered to work together toward a common goal. Organizations that are moving the fastest in this area have active Information Sharing and Analysis structures. Our state and local governments must take steps to spell out a highly coordinated approach – with clear roles and responsibilities – to enable state-wide threat visibility, consistent reporting, education, and rapid incident response procedures.

Collaboration in the States

The issues the CCoE is designed to address are not new, nor are they confined to Oregon. Other states are making this investment. Massachusetts codified in 2022 the MassCyberCenter and its mission of convening state and local officials with the private sector to address cybersecurity resiliency, cybersecurity workforce development, and overall access to cybersecurity resources. The Texas Department of Information Resources (DIR) and Angelo State University (ASU) announced in April of 2022 a Regional Security Operations Center (RSOC) designed to support the cybersecurity needs of counties, local governments, school districts, water districts, hospital districts, and regional state agency offices. Additionally, organizations like the Arizona Cyber Threat Response Alliance (ACTRA), the National Security Collaboration Center at the University of Texas at San Antonio (NSCC), and NIST's collaboration with Maryland and Montgomery County to form the National Cybersecurity Center of Excellence were all created to raise awareness, share information, and educate.

Cisco has participated in the creation of and collaboration with a number of these organizations. Some organizations thrive and others do not. For the organizations that thrive a key component is the ability for industry and government to openly collaborate. One way to enable that collaboration is to ensure a seat at the table for industry, but in a way that enables both parties to share threat intelligence, best practices, as well as lessons learned in a way that does not put either organization at risk. That requires a forum where confidential information can be shared while investigations are ongoing and in which public disclosure may enable bad actors to obfuscate or escalate their activities. To that end, the CCoE should formally enable industry to participate but that participation should not conflict the industry out of opportunities to do business in the future.

Workforce Development

Workforce development is a key component of any strategy that seeks to meet our cybersecurity challenge. Cisco's global IT skills-to-jobs program, known as Networking Academy, is one way we partner with educators to help grow the cybersecurity and technology workforce. Networking Academy is currently training Oregon's workforce online and via partnerships with a dozen high schools and community colleges throughout the state. The multilingual program has a curriculum to support educators and learners with industry-recognized skills and certifications. Since its inception, Cisco's Networking Academy has served over 15 thousand learners in Oregon and 17.5 million worldwide.

While several Networking Academy offerings are free of charge, many of the industry recognized certifications do have a fee. For our Cisco CyberOps Associate and Cisco Certified Network Associate (CCNA) certifications, we provide discount vouchers to Networking Academy students who pass their final exam with a score of 70% or greater. The discount vouchers bring down the cost to about $125 per certification in the U.S. We also provide Networking Academy curriculum completion certificates and digital badges (validated by Credly), free of charge, for students to highlight skills they've acquired and demonstrate their readiness for job roles.

In the end, the Center of Excellence is the right step forward for Oregon as we all work towards improving cybersecurity locally and statewide.

Thank you again for the opportunity to present Cisco's perspective. I welcome questions from the Committee.

Additional Resources:

2022 Talos Year in Review: https://blog.talosintelligence.com/year-in-review/
Cisco Networking Academy Cybersecurity: https://www.netacad.com/courses/cybersecurity
Cisco Networking Academy Oregon Impact: https://www.cisco.com/c/dam/en_us/about/csr/impact/education/networking-academy/fy22-pdfs/networking-academy-oregon-impact-report.pdf