HB 2049 – DRAFT Testimony Traci Esteve, Co-Chair TAO Cybersecurity Community

My name is Traci Esteve and I appreciate the opportunity to speak on behalf of HB 2049. I'm here as a US citizen, a proud Oregonian, a mother, a cybersecurity professional, an expert in Cyber Risk Management, and the Co-Chair for the Technology Association of Oregon Cybersecurity Community. My experience in Information Technology goes back to the 1980's where I was one of two women at Miami University who earned a BS in Applied Science with a major in Systems Analysis and Design (this is a combination of Computer Science, Business, and Communications). Since graduating all those years ago, I've been blessed to follow my passion of working with business, technology, and people to solve business issues and bring customer value.

My career has taken me throughout the US, to Asia, and Europe while finally discovering our incredible State of Oregon. Like all of us, Covid brought not only unique challenges, but opportunities that I took advantage of to grow my knowledge and experience. I chose to go back to school, virtually, and I obtained an MBA certification from Miami University as well as two certifications from Harvard University. One in Cybersecurity Risk Management and another in Data Privacy.

This, along with decades of experience in all aspects of Information Technology and from focusing exclusively on cybersecurity for the last eight years, has given me great cause for concern regarding the cyber risk to our nation, our state, our families and to ourselves. We need to act now, and HB 2049 will help us mitigate these risks.

I believe in this bill because I have seen the solution work. For three years, I worked for a Managed Security Service Provider of Managed Detection and Response (also known as MDR). This aligns with HB 2049's Cybersecurity Center of Excellence's cybersecurity assessment, scanning and analysis, monitoring and incident response service. One of our customer cohorts included government agencies - courts, cities, counties, and emergency services. The individual organizations were onboarded into the cohort at a reduced rate that represented their usage. Thus, making this service much more affordable than if they had to do the monitoring and detection themselves. I would like to share two stories which illustrate how a Cybersecurity Center of Excellence supporting our state can benefit from such a collaboration.

1. City Ransomware Attack - A ransomware attack is used by threat actors (individuals wishing the city harm) to lock an organization out of their own systems. We had notified this particular city of indicators of compromise (pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network) on their network. Unfortunately, they were not prepared and did not have the means or workforce to properly address these findings. As a result, several of their services were shut down and taken over by threat actors. While no individuals were physically harmed, the city spent millions recovering. While they had the MDR service, they did not have the education, procedures, training, or staff to address these types of situations in a timely manner. A Cyber Center is not enough. Education and training of staff and practiced procedures must be balanced with the technology component. On the positive side, we were able to hunt for similar indicators of compromise in other customers' environments and work together to remediate them before they were activated. These customers (also part of the government cohort) had the advantage of knowing a cyber attack had already occurred and were able to escalate the remediation.

2. City Court Zero-Day Attack - A zero-day attack occurs when a threat actor targets a software vulnerability which is unknown prior to the attack. We had a very well trained and prepared city court team who observed some minor anomalies in their email system. Per procedure, they immediately contacted us and we were able to correlate this along with other information to find the indicators of compromise and remediate the situation before the vulnerabilities were exploited. Given that there were other courts, we were able to hunt for similar indicators of compromise and stop them. Due to the teamwork, shared responsibility model, planning, and training of the courts, we were able to stop the zero-day attack without any disruption of services and our citizen's data remained secure.

HB 2049 includes not only the technology components of MDR but the other very important aspects to achieve cyber resiliency. These are the components the City Ransomware team lacked. These include:

- Awareness, education, and training
- Policies and Procedures
- Best Practices

Through understanding best practices, developing operating procedures, and educating their team, businesses (non-profits, public, or private) can address their cyber risk as business risk. Each of the risks and their mitigating controls need to be evaluated across the top three business objectives:

- Business -provide services and programs in a cost-effective manner. For public and private organizations- balancing revenue and expenses to increase profitability.
- Customer - maximize customer value.
- Regulations - effectively meet regulatory requirements.

These are often referred to as the three R's - Revenue, Reputation, and Regulation.

While businesses strive to meet these objectives, Cyber Resiliency uses a model referred to as the CIA Triangle. When these standards are met, the security posture of the business is stronger and better equipped to manage their risks and handle security incidents. The CIA Triangle includes:

- Confidentiality - protecting information from unauthorized access.
- Integrity - guarding against improper capture, modification, or destruction of information as well as against improper use, modification or destruction of systems.
- Availability - enable timely, reliable access to the use of information.

Let's break down the City Ransomware Attack example above into the Business Risk components:

Business (revenue - delivering programs and services)

- Many city services and programs were affected by the attack, including utility, parking, and court services.
- Revenue was lost as citizens were unable to pay their bills on time.
- Over $2 million dollars were spent to pay overtime and hire contractors to recover the systems.
- Over $9 million dollars were spent to rebuild the systems.
- The incident is estimated to have cost both the city and its taxpayers in excess of $12 million dollars.

Customer (the city's reputation)

- Citizens were concerned that their city was not safe.
- Given that one aspect of the city was attacked, the airports and other businesses were put on high alert.
- Approximately 6 million people were impacted.
- Citizen's data was compromised (confidential information such as court testimony was lost or exposed)
- Legal documents and police dashcam videos were permanently deleted, impacting legal services and citizen's rights.

Regulations

- Notifications to citizens and organizations impacted by the ransomware were required.
- Fines and legal actions.
- FBI and Homeland security teams were engaged.

From a Cybersecurity perspective, NONE of the cyber resiliency standards in the CIA Triangle were met - data was not kept confidential, the integrity of processing and data was compromised, and programs and services were not available.

Technology alone is not enough. The business' objectives must be understood – what are the critical programs and services? We must identify the risks to those solutions and develop and monitor them through appropriate controls. Our people must be educated and know what to do to prevent loss and protect our most valuable assets.

Thank you so much for having me today. It is an honor. As I started off my career focusing on business, computer science, and communication, I'm here to follow my passion. I am passionate about Oregon business. I am passionate about secure technology. Most importantly, I am passionate about protecting you. HB 2049 can help us accomplish this together, and we must get started now to ensure our businesses and citizens are secure.