Testimony of Anya Trundy, Deputy Commissioner
Department of Administrative and Financial Services

Testifying in Favor

LD 2092, An Act to Update Certain Terms and References Regarding Information Technology and Cybersecurity

Presented by Rep. Suzanne Salisbury

To the Joint Standing Committee on State and Local Government

Senator Baldacci and distinguished members of the Joint Standing Committee on State and Local Government. I am Anya Trundy, Deputy Commissioner of the Department of Administrative and Financial Services. I appreciate the opportunity to provide testimony in support of LD 2092, which makes meaningful and necessary updates to the statutes governing the Office of Information Technology (OIT).

As you are all aware, the information technology (IT) landscape has transformed significantly over recent years to make our world increasingly interconnected. From advancements in emerging technologies such as artificial intelligence, to the rise in sophisticated cyber threats, these changes have converged to introduce both new opportunities and new challenges to State Government services and operations. Given the speed of innovation and the dynamic nature of the cyber threat environment, OIT has evolved to meet these challenges, striving to balance innovation and risk in the delivery of reliable, secure and effective technology solutions for state agencies and Maine residents.

Unprecedented growth in emerging technologies, such as artificial intelligence, and a dramatic increase in cyber threats, have resulted in a host of new federal and state data protection laws and regulations. As a result, the statute governing the State's use of technology requires amending to keep pace and accurately reflects OIT's present day mission and ensure compliance with best practices.

This bill would accomplish five main objectives:

First, it provides the CIO with authority to appoint an authorized designee in specific situations. In recent years, the CIO's role and responsibilities have grown significantly. The ability to delegate authority to direct reports with applicable expertise and responsibility will help streamline operations and maximize the CIO's efforts in managing new areas within the organization (*see sections 12, 13, 14 and 15 of the bill*).

Second, the bill makes important updates to definitions to align with the recently enacted definition of "cyberattack" within the Department of Public Safety's statutes and adds definitions for cybersecurity and information security that are reflective of national best practices (*see sections 7, 9 of the bill*).

Third, it updates language regarding the vision and mission of OIT to reflect updates in terminology and best practices for safeguarding the confidentiality, integrity and availability of the State's information and communications technology infrastructure, systems and services against emerging threats (*see section 5, 10 and 16 of the bill*).

Fourth and most substantially, the bill updates the statute to remove barriers in OIT's ability to detect, prevent, and respond to cyberattacks (*see sections 4 and section 15 of the bill).* Absent these changes, OIT lacks the ability to procure cyber incident response retainers – a crucial tool

for mitigating risk and ensuring an effective response to cyber incidents. This bill makes it possible for OIT to have the capacity for a swift and coordinated response to cyber incidents, bringing its framework into alignment with best practices. The key benefits of cyber retainers include:

- **Industry Best Practices** – Public sector entities are increasingly adopting cyber retainers to effectively handle complex and frequent cyber threats. These services help speed up remediation, ensure regulatory compliance, minimize unauthorized data access, and quickly repair IT damage. Retainer services are more cost-effective than maintaining in-house capabilities that may not be needed regularly. Engaging cyber services on retainer allows for the identification of the most cost-effective solution, rather than hastily securing services during an active cyberattack.
- **Accelerated Incident Response** – Quick response is crucial during a cyber incident to reduce data loss, financial damage, and reputational harm. With retainer services, the State would have expert teams on hand, prepared to respond with knowledge about the State's unique IT infrastructure, helping to minimize valuable response time and avoid costly mistakes.
- **Ongoing Preparedness and Prevention** – Retainers provide targeted and timely preparedness services like penetration testing, threat intelligence, forensic tools, security architecture, crisis communications, and simulated attack exercises.
- **Protecting Reputation and Building Trust** – Proactive cyber measures show the State's commitment to mitigating risks to sensitive citizen data and critical IT infrastructure.

Lastly, this bill removes unintended barriers in procurement that make federal General Services Administration (GSA) procurement programs inaccessible to the State (see section 3 of the bill). GSA procurement programs are open to state and local governments across the country, providing access to specialized, cost-effective, high value IT tools and services that leverage the benefit of federal buying power. Companies that participate in GSA programs must be compliant with stringent federal regulations (compliance with the FAR, the FCC Covered list, Section 889 of the National Defense Authorization Act, as well as other federal information security regulatory requirements). This bill will allow OIT to gain access to these programs, offering significant advantages, from saving time and taxpayer money to ensuring access to reliable, high-quality IT products and services with standardized pricing, simplified processes, and thousands of vetted contractors.

This bill brings OIT's statute into alignment with the modern day to more accurately reflect current IT terminology and removes outdated language that impedes our State's cyber readiness. Most importantly, this bill will bridge the gap to ensure that advancements in technology, including cybersecurity, are accurately reflected in OIT's statute.

For these reasons, I urge you to support LD 2092. Thank you for your consideration of this bill, I am happy to answer questions and will be available at the work session.