SB 293 STAFF MEASURE SUMMARY

Carrier: Rep. Nathanson

Joint Committee On Information Management and Technology

Action Date:	05/19/21
Action:	Do Pass.
House Vote	
Yeas:	3 - Marsh, Nathanson, Post
Senate Vote	
Yeas:	2 - Johnson, Riley
Exc:	1 - Boquist
Fiscal:	Has minimal fiscal impact
Revenue:	No revenue impact
Prepared By:	Sean McSpaden, Committee Coordinator
Meeting Dates:	3/31, 5/19

WHAT THE MEASURE DOES:

Directs office of the State Chief Information Officer (CIO) to prepare recommendations for elevating consideration of privacy, confidentiality and data security measures in the design, delivery and management of enterprise and shared information technology services for state government, and submit recommendations in a report to interim committees of Legislative Assembly related to government accountability and information technology by September 15, 2022. Under the measure, the recommendations shall consider and address (among other topics), the merits of either establishing and appointing a dedicated state privacy officer within the office of the State CIO to manage and oversee information protection and privacy guidance for state government, or continuing to delegate such duties to the Chief Data Officer, established via HB 3361 (Chapter 720, 2017 Laws), or another officer within the office's current management team. The measure would take effect on 91st day following adjournment sine die and sunset on January 2, 2023.

ISSUES DISCUSSED:

- Potential impact on the measure due to the recent name change for office of the State Chief Information Officer

EFFECT OF AMENDMENT:

No amendment.

BACKGROUND:

Per ORS 276A.300, the State Chief Information Officer (CIO) has responsibility for and authority over information systems security in the executive department (except for the Secretary of State, State Treasurer, and the Attorney General per ORS 276A.303), including responsibility for taking all measures that are reasonably necessary to protect the availability, integrity or confidentiality of information systems or the information stored in information systems. Under State IT Policy - 107-004-052 (Cyber and Information Security - November 2020) - Information Security is defined as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability. Under that policy, confidentiality, integrity and availability are defined as follows:

- Confidentiality: The principle of preserving authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information.
- Integrity: The principle of guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.
- Availability: The principle of ensuring timely and reliable access to and use of information.

Although not statutorily required, the State CIO has established a position within the office of the State CIO, and has appointed and delegated these responsibilities to an individual who serves as the State Chief Information Security Officer.

Under State IT Policy - 107-004-050 (Information Asset Classification - January 2008), executive branch state agencies are (among other things) required to develop a plan for identifying, classifying and protecting information assets according to classification framework outlined within the policy, and to properly identify and protect information meeting the definitions, requirements and effective dates outlined within ORS 646A.600 to 646A.628 (the Oregon Consumer Information Protection Act) as they relate to personal information.

ORS 276A.353 directed the State CIO to appoint a Chief Data Officer (CDO) who shall (among other duties):

- Establish an open data standard, and prepare and publish a technical standards manual.
- Create an enterprise data inventory that accounts for all datasets used within agency information systems and that indicates whether each dataset may be made publicly available and if the dataset is currently available to the public.
- Provide information protection and privacy guidance for state agencies.
- Establish an enterprise data and information strategy.
- Establish statewide data governance and policy area data governance and provide guidance for agencies about data governance efforts.
- Oversee the delivery of education and standards to state agencies regarding data quality, master data management and data life cycle management.

In November 2020, the Secretary of State published audit report 2020-37. The purpose of this enterprise data privacy risk audit was to assess whether Oregon has a governance structure in place to manage the risks to data privacy for the personally identifiable information (PII) it collects. Among other things, the audit report found that:

- Oregon does not have a statewide official responsible or accountable for managing data privacy risk.
- The office of the State CIO has not provided agencies with clear guidance on how to respond to a security incident involving PII.
- Though still developing foundational policy and strategy, the CDO has made progress in implementing enterprise data governance requirements.

Within the audit report, the Secretary of State audit team recommended that the State CIO request funding to establish a statewide privacy office and appoint a Chief Privacy Officer (CPO), or similar role, whose position will have the authority, mission, accountability, and resources to coordinate and develop statewide privacy requirements. The SOS audit team further recommended that the CPO be charged with the following tasks:

- Develop a strategic plan and timeline for coordinating an enterprise privacy risk assessment, developing statewide policies and procedures to manage and monitor privacy risk, and providing privacy training to agency personnel and third parties engaged in data processing.
- Work with other state officials as necessary to ensure roles for responding to incidents involving PII are clearly and consistently articulated in statewide policies, procedures, and plans.
- Once roles are clearly established, work with other state officials as necessary to ensure incident response training is provided to agency personnel consistent with assigned roles and responsibilities.