SB 1073 A STAFF MEASURE SUMMARY

Joint Committee On Information Management and Technology

Action Date:	04/05/23
Action:	Do pass with amendments. Refer to Ways and Means by prior reference. (Printed A-Eng).
Senate Vote	
Yeas:	2 - Thatcher, Woods
Exc:	1 - Taylor
House Vote	
Yeas:	2 - Hartman, Nathanson
Exc:	1 - Mannix
Fiscal:	Fiscal impact issued
Revenue:	No revenue impact
Prepared By:	Sean McSpaden, Committee Coordinator
Meeting Dates:	3/22, 4/5

WHAT THE MEASURE DOES:

Senate Bill 1073 directs the State Chief Information Officer to appoint a Chief Privacy Officer and describes the scope of duties of the Chief Privacy Officer. Among other duties, the measure directs the Chief Privacy Officer to conduct a biennial executive branch privacy assessment, and to develop and conduct privacy trainings for state agencies and employees.

Senate Bill 1073 directs the Chief Privacy Officer and the Chief Data Officer, described within ORS 276A.353, to coordinate activities within their respective areas of responsibility. The measure further directs state agencies to designate agency data officers and directs the Chief Privacy Officer to coordinate data privacy activities with those agency data officers.

Finally, Senate Bill 1073 section 1(4) excludes the Secretary of State and the State Treasurer from the definition of a "state agency" within the executive department and directs the Secretary of State and State Treasurer to independently adopt by rule certain data privacy requirements, ensuring they are the same as, or are similar to, the requirements established by, and rules adopted by the State Chief Information Officer under section 1 of this 2023 Act.

ISSUES DISCUSSED:

- Various aspects of the proposed amendment
- SB 293 (2021) - State Chief Information Officer recommendations on the merits of establishing a dedicated Oregon chief privacy officer, developing a privacy assessment tool, and the need for education, outreach and training on privacy within Oregon state government.
- Consumer privacy legislation and regulations considered or established across the country.
- Federal requirements for information security and privacy.
- FIPPS - Fair Information Practice Principles established by the Federal Privacy Council: Access and Amendment; Accountability; Authority; Minimization; Quality and Integrity; Individual Participation; Purpose Specification and Use Limitation; Security; and Transparency.
- Complementary roles and responsibilities of Oregon's Chief Information Security Officer, Chief Data Officer, and (potentially) a newly created Chief Privacy Officer position.
- Funding and staff resources required to establish a Chief Privacy Officer position and program.
- Need for Chief Privacy Officer to report regularly to the legislature on privacy program activities and progress.
- Privacy and its relationship to transparency. Expectation of transparency and data sharing among and between public bodies and with the public, unless explicit information security and privacy statutes, rules, policies, or regulation prevent that from occurring. Need for standardized privacy practices.

- Department of Justice support for the measure and request for amendments.
- Expectation that the Secretary of State, State Treasurer, and the Attorney General develop privacy related strategies, policies, and standard practices for their offices that mirror and align with those established by the State Chief Information Officer for state agencies within the executive department.
- Other information security and privacy legislation being considered during the 2023 legislative session - e.g. HB 2049, HB 2052, HB 2490, HB 2806, HB 3127 and SB 619.
- League of Women Voters support for the measure. Need for local government education, training, and communication forums.

EFFECT OF AMENDMENT:

The amendment directs the Chief Privacy Officer to submit a biennial report to a committee or interim committee of the Legislative Assembly related to information management and technology and specifies the content of that report.

The amendment modifies the definition proposed for "state agency" and "executive department" in SECTION 1(4) to exempt, and maintain the independent authorities of, the Attorney General along with the Secretary of State and the State Treasurer.

The amendment requires the Attorney General, along with the Secretary of State and the State Treasurer, to by rule adopt for each respective office requirements related to data privacy that are the same as, or are similar to, the requirements established by this 2023 Act and by rules adopted the State Chief Information Officer for state agencies within the executive department.

BACKGROUND:

Secretary of State Audit Report (2020-37), entitled - Department of Administrative Services (DAS) Enterprise Information Services (EIS) - The State Does Not Have A Privacy Program to Manage Enterprise Data Privacy Risk, found that:

- Oregon does not have a statewide official responsible or accountable for managing data privacy risk.
- Enterprise Information Services (EIS) has not provided agencies with clear guidance on how to respond to a security incident involving PII; and
- Though still developing foundational policy and strategy, the Chief Data Officer has made progress in implementing enterprise data governance requirements.

Within the report, the Secretary of State (SOS) audit team recommended that DAS EIS request funding from the Legislative Assembly to establish a statewide privacy office and appoint a senior official responsible for managing an enterprise privacy program. Additionally, the SOS audit team recommended that DAS EIS should clarify roles and provide training to ensure agency personnel understand their role in responding to incidents involving Personally Identifiable Information.

During the 2021 Legislative Session, Senate Bill 293 was introduced and passed into law. Senate Bill 293 (2021) directed DAS EIS (previously known as the office of the State Chief Information Officer) to develop recommendations related to elevating consideration of privacy, confidentiality and data security measures in state government enterprise and shared information technology services, and to submit recommendations in a report to certain interim committees of Legislative Assembly by September 15, 2022. The report was delivered as required and recommended the following for addressing privacy within Oregon state government:

1. Establish a Chief Privacy Officer role reporting to the State Chief Information Officer (CIO) within EIS and build an Enterprise Privacy Program.
2. Require the Chief Privacy Officer to develop and implement an Enterprise Privacy Program for the state of Oregon and make recommendations to the State CIO regarding appropriate privacy program models (e.g., centralized, hybrid, decentralized) for adoption.
3. Create statutory authorization and budgetary authority for the Chief Privacy Officer. EIS recommended adopting legislation identifying the roles and responsibilities of a Chief Privacy Officer in relation to other roles

within the state, such as the Chief Data Officer, and outlining core expectations for state agencies in managing privacy risk.

4. Establish Privacy Program deliverables. The Chief Privacy Officer should be tasked with development of an enterprise privacy risk assessment and a privacy assessment tool or similar resource to allow agencies to evaluate and manage privacy risk. EIS recommended the Chief Privacy Officer develop enterprise privacy guidance and a privacy risk assessment approach in advance of incorporating privacy impact assessments or other evaluative frameworks into the state's current information technology oversight process. The Chief Privacy Officer should utilize this assessment as a baseline to develop further recommendations related to incorporating privacy considerations at the IT project level.
5. Develop privacy outreach, education, and engagement strategies for the public. Utilize both the Chief Privacy Officer's and Chief Data Officer's unique expertise in the areas of open data, data use, privacy, and privacy rights to develop an education and engagement strategy for those whose information is collected, stored, compiled, or otherwise used as part of a state agency project, program, or IT investment.

DAS EIS has submitted a policy option package to establish a Chief Privacy Officer position and program as part of the Governor's Budget Request for the 2023-25 biennium. That request is being considered by the Joint Committee on Ways and Means.