SB 1073 STAFF MEASURE SUMMARY

Joint Committee On Information Management and Technology

Prepared By:	Sean McSpaden, Committee Coordinator
Sub-Referral To:	Joint Committee On Ways and Means
Meeting Dates:	3/22

WHAT THE MEASURE DOES:

Senate Bill 1049 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 1049 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:

EFFECT OF AMENDMENT:

No amendment.

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.