Oregon
Kate Brown, Governor

Department of Administrative Services
Enterprise Information Services (EIS)
155 Cottage Street NE
Salem, OR 97301-3972
PHONE: 503-378-2349
FAX: 503-373-1273

March 26, 2021

Senator Chuck Riley, Co-Chair
Representative Nancy Nathanson, Co-Chair
Joint Committee on Legislative Information Management and Technology
900 Court Street NE
H-170 State Capitol
Salem, OR 97301-4048

RE: Invited Testimony on SB 293 (2021) – directing EIS to develop recommendations for elevating considerations of privacy, confidentiality, and data security within shared and enterprise information technology services

Dear Co-Chairpersons:

Enterprise Information Services (EIS) appreciates the opportunity to provide written testimony on SB 293 (2021), a measure that would direct EIS to develop recommendations on the merits of establishing a dedicated state privacy officer within EIS, embedding privacy assessments within the oversight of information technology (IT) investments, and conducting privacy-related outreach, education, and engagement on behalf of the people of Oregon. While EIS is neutral on SB 293, we appreciate the Committee's continued leadership on the issue of data privacy and acknowledge the need for dedicated privacy leadership within state government.

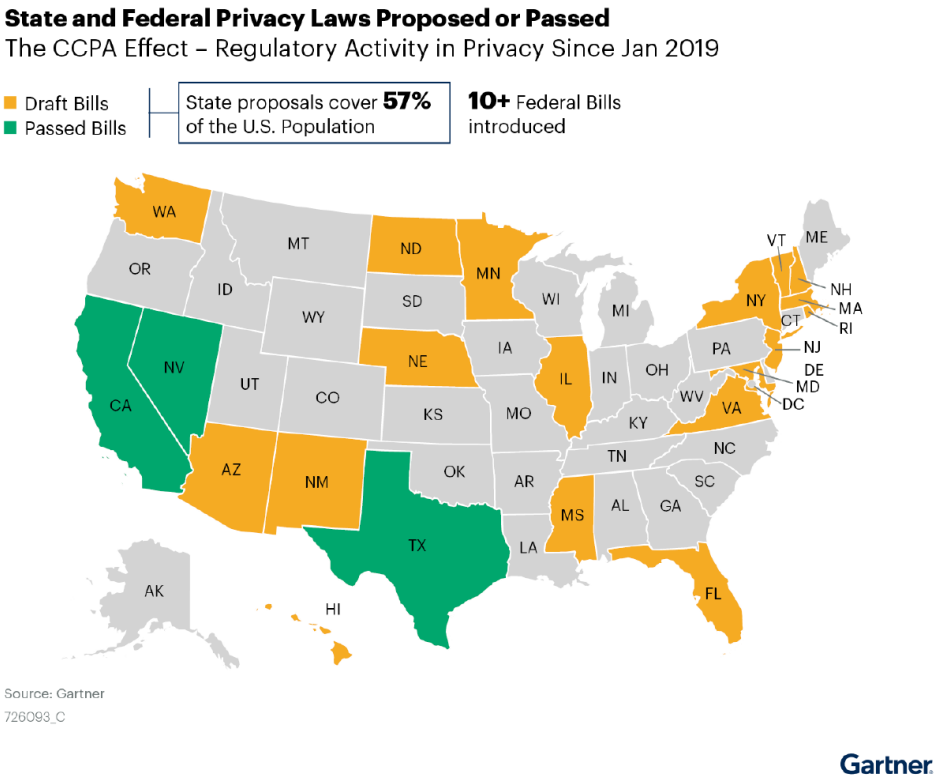
The need for such privacy leadership was identified in the recent Secretary of State Audit Report 2020-37, *Department of Administrative Services and Enterprise Information Services, The State Does Not have a Privacy Program to Manage Enterprise Data Privacy Risk.* The Secretary of State's sole audit recommendation to EIS is excerpted below.

1. *Request funding to establish a statewide privacy office and appoint a Chief Privacy Officer, or similar role, whose position will have the authority, mission, accountability, and resources to coordinate and develop statewide privacy requirements. Charge the CPO with the following tasks:*
    a. *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;*
    b. *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; and*
    c. *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.*

As previously described in our audit response and in informational testimony provided to this Committee on March 3, 2021, EIS agrees with this recommendation, having previously developed a

draft legislative concept (LC) to establish a Chief Privacy Officer (CPO) within EIS and provide the requisite authority for rulemaking and agency guidance; however, as previously noted, the proposed LC was not introduced due to anticipated budgetary constraints for the 21-23 biennium.

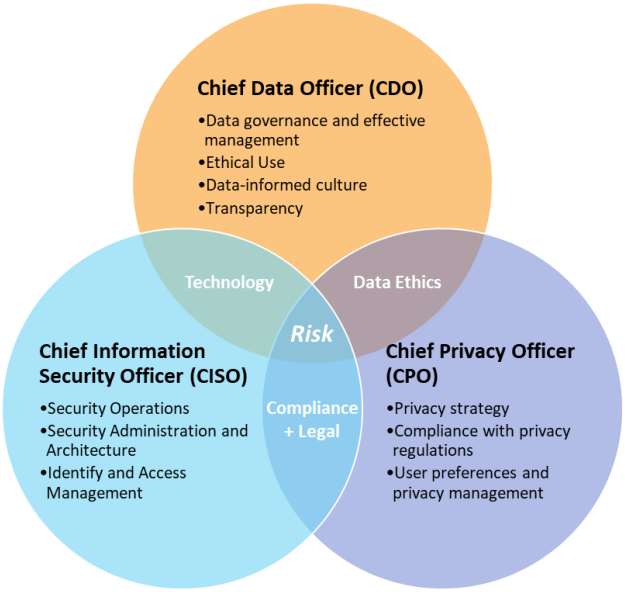
By way of background and as noted within the audit, there is currently no authoritative definition of *"data privacy,"* or *"personally identifiable information"* given the absence of comprehensive federal regulation or single statewide privacy law within Oregon. Rather, the US model of privacy protection has evolved in a sectorial manner and in response to the needs of specific industries or vulnerable population segments and is better characterized as an increasingly complex patchwork of narrowly-tailored Federal statutes (e.g., Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA)), judicial decisions, and state-level privacy laws.



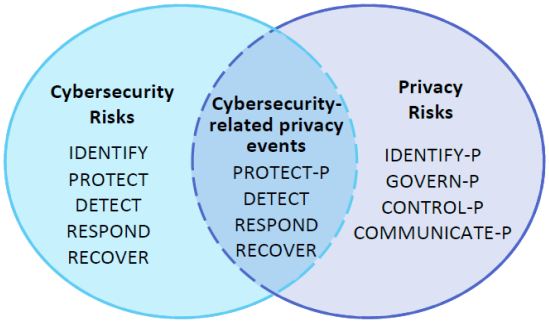
The passage of the California Consumer Privacy Act (CCPA) in 2018 exemplifies these state-level efforts and has been followed by a flood of CCPA-inspired state legislation—what Gartner has termed the "CCPA Effect." As of January 2021, Gartner reported that more than 10 states had introduced CCPA-inspired laws (in some cases, exceeding the scope of the CCPA) that taken together would cover 57% of the US population. Earlier this month, the State of Virginia became the latest state to pass comprehensive privacy legislation, with Governor Ralph Northam signing the Virginia Consumer Protection Act (S.B. 1392) into law on March 3, 2021. Suffice to say, the national privacy landscape continues to evolve rapidly.

Given this rapidly evolving and increasingly complex regulatory environment coupled with increased public concern over the collection, use, dissemination, protection, destruction, and use of citizen data, both private- and public-sector leaders have recognized the need for privacy leadership through the appointment of Chief Privacy Officers (CPOs) and establishment of data

privacy programs. A trend documented by NASCIO in its March 2019 report, *Perspectives on Privacy: A Survey and Snapshot of the Growing State Chief Privacy Officer Role.* By the beginning of 2019, NASCIO reported that 12 states had established a CPO or equivalent position—with more likely to follow.

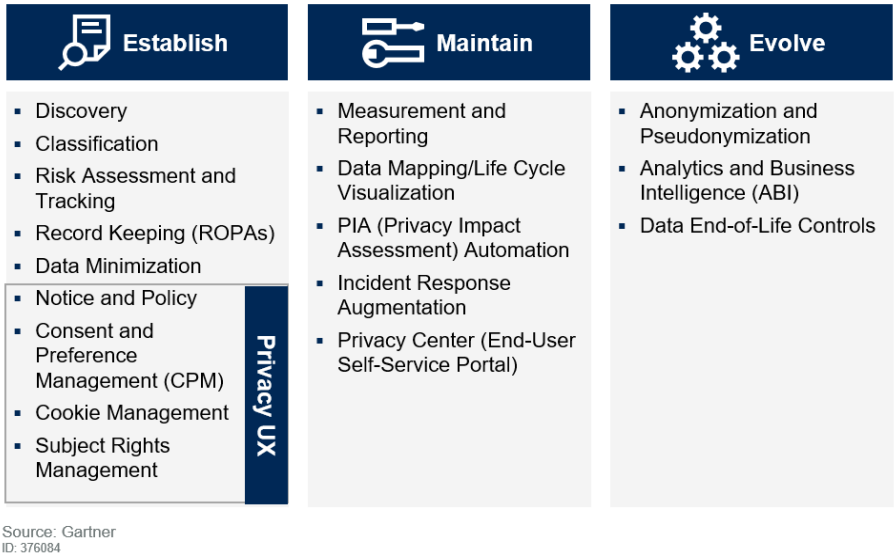


Given the close relationship between data governance, information security, and data privacy, there is a tendency to conflate the roles of Chief Data Officers (CDOs), Chief Information Security Officers (CISOs), and Chief Privacy Officers (CPOs). While these related roles share responsibility for data risk, the three roles represent separate disciplines. Public-sector CDOs are focused on data governance and effective management, ethical use, building a data-informed culture, and data transparency. In other words, how do we leverage the data entrusted to the State of Oregon as a strategic asset? Whereas CISOs are focused on security operations, administration, architecture, identity, and access management. In effect, how do we protect and manage access to the state's data assets through physical, technical, and administrative controls? By contrast, CPOs are primarily focused on regulatory and legal compliance. Put differently, how do we manage risk associated with the collection, storage, and management of data?



The data privacy/information security distinction is explicitly addressed within the NIST Privacy Framework, Version 1.0. In effect, privacy and security represent categories of risks that may or may not overlap within the context of a single "privacy event"—such an event may result from

normal "data processing" rather than an incident impacting the confidentiality, availability, or integrity of data.



Beyond the privacy/security distinction and differentiation of operational responsibilities between CDOs, CISOs, and CPOs, the effective management of privacy risk within Oregon state government will require dedicated leadership, a comprehensive privacy strategy, the development of statewide policies and procedures, the establishment of programmatic capabilities (see examples above), and adequate resourcing—both within EIS and our partner agencies across the Executive Branch. It is difficult to overstate the vital role of our partner agencies, given their data collection activities and amassing of data from innumerable constituents across multiple contexts. Ultimately, it is our partner agencies that are responsible for effectively stewarding and protecting the people of Oregon's data that they hold in trust.

In closing, we appreciate the Committee's continued leadership on the issue of data privacy and welcome the opportunity to discuss these important issues further.

Sincerely,

Terrence Woods
State Chief Information Officer

Cc: Sean McSpaden, Legislative Fiscal Office
Laurie Byerly, Legislative Fiscal Office