SB 293 (2021) ENTERPRISE PRIVACY

ENTERPRISE INFORMATION SERVICES' RECOMMENDATIONS FOR ELEVATING CONSIDERATIONS OF PRIVACY, CONFIDENTIALITY, AND DATA SECURITY

SEPTEMBER 2022

ENTERPRISE
information services

Contents

Executive Summary

Enterprise Information Services (EIS) was charged by Senate Bill (SB) 293 (2021) 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. In preparing the recommendations EIS considered:

a) The merits of either establishing and appointing a dedicated state privacy officer within EIS to manage and oversee information protection and privacy guidance for state government, or continuing to delegate such duties to the Chief Data Officer or another officer within the EIS' current management team;

b) The merits of developing and embedding a robust privacy assessment tool within existing evaluative frameworks for state government information technology projects and investments; and

c) The merits of outreach, education and engagement with those whose information is collected, stored, compiled, utilized, commodified or otherwise used as part of a state agency information technology project or investment.

Problem Statement

Given the emergent trend of increased public concern over the collection, use, protection, and destruction of citizen data, both private- and public-sector leaders have recognized the need for privacy leadership through the appointment of Chief Privacy Officers and establishment of data privacy programs. In recent years, there has been an unprecedented increase in demand for privacy professionals. It is estimated that half a million organizations have appointed at least one privacy officer since 2018.[1] By the beginning of 2019, The National Association of State Chief Information Officers (NASCIO) reported 12 states had established a Chief Privacy Officer.[2] In a 2022 update to the report, NASCIO reported 21 states have a state Chief Privacy Officer role or equivalent.[3]

Despite these global and national trends, the state of Oregon does not have an enterprise approach to privacy or identified privacy leadership. Absent privacy leadership statewide or within Executive Branch agencies, Oregon will lose further ground relative to other states and continue to accrue substantial privacy risk. This absence of privacy leadership and in-house privacy expertise leaves the Executive Branch at a disadvantage within the context of policy development and legislative deliberations regarding data privacy issues more broadly and severely limits the administrative feasibility of implementing new privacy regulations or requirements as they are developed, either statewide or federally.

Process Summary

EIS has undertaken a close analysis of different opportunities to address enterprise privacy risk, including best practices within other states, and recommendations from Gartner, Info-Tech Research Group, and the International Association of Privacy Professionals.

---

[1] Henein, Nader, and Bart Willemsen. "The Privacy Officer's First 100 Days." Gartner, April 15, 2019.
[2] Glasscock, Amy Hille. "Perspectives on Privacy: A Survey and Snapshot of the Growing State Chief Privacy Officer Role." NASCIO, March 27, 2019. https://www.nascio.org/resource-center/resources/perspectives-on-privacy-a-survey-and-snapshot-of-the-growing-state-chief-privacy-officer-role/.
[3] Glasscock, Amy Hille. "Privacy Progressing: How the State Chief Privacy Officer Role is Growing and Evolving." NASCIO, June 15, 2022. https://www.nascio.org/resource-center/resources/privacy-progressing-how-the-state-chief-privacy-officer-role-is-growing-and-evolving/

Enterprise Information Services also engaged in conversations with key stakeholders in technology and policy to vet and provide guidance on the recommendations reported below. This stakeholder feedback was incorporated in the crafting of EIS recommendations.

Recommendations

In response to the growing need for enterprise privacy leadership and the direction of SB 293, EIS reports the following recommendations for addressing privacy within the state of Oregon 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 recommends 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 recommends 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.

These recommendations are consistent with the findings in the 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 audit contains a sole recommendation that EIS "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."[4]

[4] Oregon Secretary of State Audits Division. *The State Does Not Have a Privacy Program to Manage Enterprise Data Privacy Risk*. November 2020. http://records.sos.state.or.us/ORSOSWebDrawer/Recordhtml/7672528

Overview

Senate Bill 293

The 2021 Oregon Legislative Assembly directed Enterprise Information Services (EIS) 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.

As guided by Senate Bill 293, EIS considered the following in preparing recommendations:

a) The merits of either establishing and appointing a dedicated state privacy officer within EIS to manage and oversee information protection and privacy guidance for state government, or continuing to delegate such duties to the Chief Data Officer or another officer within the EIS' current management team;

b) The merits of developing and embedding a robust privacy assessment tool within existing evaluative frameworks for state government information technology projects and investments; and

c) The merits of outreach, education and engagement with those whose information is collected, stored, compiled, utilized, commodified or otherwise used as part of a state agency information technology project or investment.

Discovery Process

EIS has undertaken a close analysis of different opportunities to address enterprise privacy risk, including best practices within other states and recommendations from Gartner, Info-Tech Research Group, and the International Association of Privacy Professionals. This analysis included time spent in consultant calls to learn about emerging and best practices, policy review and discussion with privacy leaders.

As part of the process for vetting and refining the recommendations presented within this report, EIS engaged in conversations with external stakeholder groups, including the Technology Association of Oregon and the League of Women Voters, to hear constituent feedback about EIS' recommendations and proposed approach to managing enterprise privacy risk. These conversations were used to further enhance EIS' primary recommendations related to creation of a Chief Privacy Officer role and in the recommendations related to privacy program deliverables. In receiving stakeholder feedback, EIS received overwhelming support for the necessity of a dedicated Chief Privacy Officer role at the state level, with stakeholders providing additional feedback regarding the need to provide preliminary staffing support and budgetary authority to a Chief Privacy Officer to ensure the role's continued success and sustainability.

Background

Enterprise Information Services Privacy Activities

Per ORS 276A.300, the State Chief Information Officer (CIO) has responsibility for and authority over information system security in the Executive Branch (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 Statewide 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 EIS and has appointed and delegated these responsibilities to an individual who serves as the State Chief Information Security Officer.

Under Statewide IT Policy 107-004-050 (Information Asset Classification – 2008)[5], Executive Branch agencies are, among other things, required to develop a plan for identifying, classifying and protecting information assets according to the 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 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 support of ORS 276A.353, EIS and the Chief Data Officer has produced Open Data Guidance: Privacy for Open Datasets, which incorporates a risk-benefit analysis process to evaluate the associated risk for publishing data as an open dataset. This privacy guidance was adopted as part of Oregon's Open Data Program to support agencies in the process of evaluating privacy risk as part of their processes for publishing open data and includes a glossary of de-identification approaches and tools to better enable agencies to manage data privacy risk as they seek to increase government transparency.

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.
- EIS 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 Chief Data Officer has made progress in implementing enterprise data governance requirements.

Within the audit report, the Secretary of State audit team recommended the State CIO 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

[5] To be consistent with updated definitions of Personally Identifiable Information within the Oregon Consumer Information Protection Act (OCIPA), EIS has drafted and is in the process of reviewing an update to the State's Information Asset Classification policy, anticipated December 2022.

requirements. The Secretary of State audit team further recommended the Chief Privacy Officer 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.

As previously stated in EIS' audit response and EIS testimony provided to the Joint Committee on Information Management and Technology on March 3, 2021, EIS agrees with this audit recommendation, having previously developed a draft legislative concept to establish a Chief Privacy Officer within EIS and provide the requisite authority for rulemaking and agency guidance; however, the proposed legislative concept was not introduced due to anticipated budget constraints for the 2021-23 biennium. EIS has updated and submitted the legislative concept request for the 2023-25 biennium.

A Rapidly Evolving Privacy Landscape

The International Association of Privacy Professionals (IAPP) defines information privacy as "the right to have some control over how your personal information is collected and used."[6] However, given the absence of comprehensive federal privacy regulation, there is currently no authoritative definition of *"data privacy," "data protection,"* or *"information privacy"* under United States law. Rather, the United States 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 judicial decisions, state law, and narrowly-scoped and specialized federal statutes."[7] The partial list of federal statutes below exemplify the fragmentary nature of United States privacy law as it currently stands.

- ***Healthcare Data***. Health Insurance Portability and Accountability Act (HIPPA)
- ***Children***. Children's Online Privacy Protection Act (COPPA)
- ***Access to Education Records***. Family Educational Rights and Privacy Act (FERPA)
- ***Financial Institutions.*** Gramm-Leach-Bliley Act (GLBA)

By contrast, Europe recognized privacy as a fundamental human right in 2000 as part of the European Union Charter of Fundamental Rights and further affirmed a right to privacy with the passage and implementation of the General Data Protection Regulation (GDPR) in 2018.[8] As of 2019, there are 132 jurisdictions that have established similar data privacy/protection laws—typically providing rights of disclosure (*i.e.,* what data is being collected) and erasure (*i.e.*, the right to fix such data or be forgotten).[9] Among these jurisdictions, 60 countries had introduced or enacted so-called "post-modern" privacy and data protection laws, including: Argentina, Brazil, Egypt, India, Indonesia, Japan, Kenya, Mexico, Nigeria, Panama, Singapore and Thailand.[10]

---

[6] "What Is Privacy." International Association of Privacy Professionals (IAPP). Accessed March 9, 2020. https://iapp.org/about/what-is-privacy/.
[7] O'Brien, Danny. "Data Privacy or Data Protection Day? It's a Human Right, Either Way." Electronic Frontier Foundation, January 29, 2020. https://www.eff.org/deeplinks/2020/01/data-privacy-or-data-protection-day-its-human-right-either-way
[8] Ibid.
[9] Ibid.
[10] Willemsen, Bart, and Nader Henein. "Predicts 2020: Embrace Privacy and Overcome Digital Ambiguity to Drive Digital Transformation." Gartner, November 14, 2019.

Privacy observers anticipate these trends will only continue to accelerate. In *Predicts 2020: Embrace Privacy and Overcome Ambiguity to Drive Digital Transformation,* Gartner anticipates:

- "Before year-end 2023, more than **80% of companies** worldwide will be facing at least one privacy-focused data regulation."
- "By 2023, **65% of the world's population** will have its personal information covered under modern privacy regulations, up from 10% today."
- "By year-end 2022, more than **1 million organizations** will have appointed a privacy officer (or data protection officer)."
- "Through 2022, privacy-driven spending on compliance tooling will break over **$8 billion worldwide.**" [11]

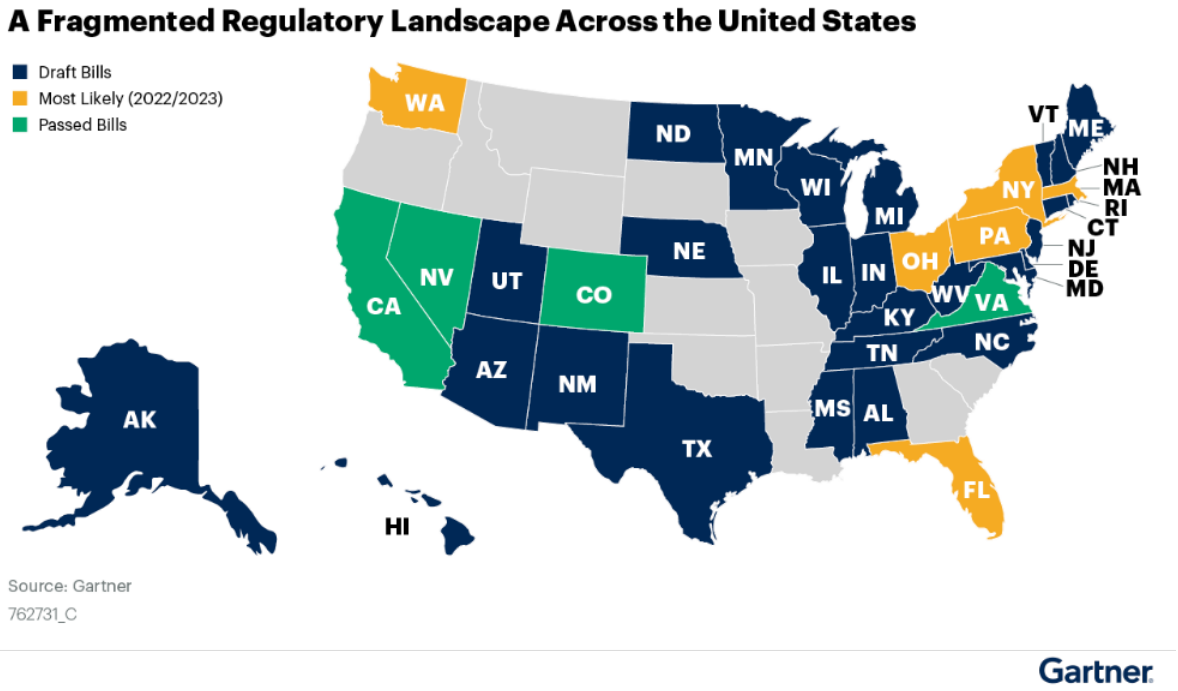
Back in the United States, the continued erosion of personal privacy, loss of trust and increasing customer dissatisfaction—be it from security breaches or the misuse of customer data (e.g., the Cambridge Analytica revelations)—has motivated federal legislators to propose new data privacy and protection laws. At the federal level, several bills have been introduced that would incorporate components of the GDPR; however, there are still substantial questions regarding the scope of these federal proposals in terms of individual rights, potential preemption of state laws, and enforcement.[12] Absent comprehensive federal legislation, Gartner anticipates efforts at the state level will only continue to accelerate, increasing regulatory complexity, fragmentation, confusion, conflicting requirements, and inconsistent enforcement at the federal level and among state's attorney generals.[13]

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/GDPR-inspired state legislation—what Gartner has termed the "CCPA Effect."[14] As of February 2022, Gartner reported that more than 35 states are seeking to develop privacy legislation, representing more than 85% of the United States population.[15] Given this CCPA Effect and the growing number of privacy regulations being introduced at the state level, it is only a matter of time before CCPA-inspired legislation is introduced in Oregon. As Figure 1 below indicates, several states have introduced or plan to introduce privacy regulations in either 2022 or 2023.

---

[11] Ibid.
[12] Willemsen, Bart. "Hype Cycle for Privacy, 2019." *Gartner*, July 11, 2019.
[13] Ibid.
[14] Henein, Nader, and Willemsen Bart. "The State of Privacy and Personal Data Protection, 2019-2020." *Gartner*, April 15, 2019.
[15] Henein, Nader, Woo, Bernard, and Willemsen Bart. "State of Privacy – Regional Overview Across North America." *Gartner*, February 4, 2022.

Figure 1. The CCPA Effect—Privacy Regulations Introduced by State[16]



Given these emergent trends; i.e., increased public concern over the collection, use, dissemination, protection, destruction, and use of citizen data coupled with a rapidly evolving and increasingly complex regulatory environment, both private- and public-sector leaders have recognized the need for privacy leadership through the appointment of Chief Privacy Officers and establishment of data privacy programs. While Chief Privacy Officers have existed within the private sector since the 1990s, the public sector has been slower to embrace the role of Chief Privacy Officer. West Virginia appointed the first state Chief Privacy Officer in 2003.[17] However, in recent years, there has been an unprecedented increase in demand for privacy professionals and it is estimated that half a million organizations have appointed at least one privacy officer since 2018,[18] 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.*[19] By the beginning of 2019, NASCIO reported that 12 states had established a Chief Privacy Officer or equivalent position.[20] In a 2022 update to the report, NASCIO reported that 21 states have a state Chief Privacy Officer role or equivalent.[21]

Despite these global and national trends, the state of Oregon still lags in terms of privacy leadership—both within individual agencies and across the Executive Branch. As part of a broader assessment of information security capabilities within EIS Cyber Security Services (CSS) and across Executive Branch agencies, Gartner found substantial gaps in privacy capabilities.[22] Specifically, Oregon lacks a statewide Chief Privacy Officer

---

[16] Ibid.
[17] Glasscock, "Perspectives on Privacy."
[18] Henein, Nader, and Bart Willemsen. "The Privacy Officer's First 100 Days." Gartner, April 15, 2019.
[19] Glasscock, "Perspectives on Privacy."
[20] Ibid.
[21] Glasscock, "Privacy Progressing."
[22] "Information Security Management Capabilities Model, Observations and Recommendations." *Gartner*, February 10, 2020.

and comparable positions only exist within one Executive Branch agency, the Oregon Department of Human Services. Additionally, Gartner found that neither CSS nor any agencies had developed "Data Breach Policy and Procedures" or established a "Privacy Impact Assessment (PIA) Process." Absent privacy leadership statewide or within Executive Branch agencies, Oregon will lose further ground relative to other states and continue to accrue substantial privacy risk.

Recommendations for Managing Enterprise Privacy Risk

Recommendation: Establish a Chief Privacy Officer and Build an Enterprise Privacy Program

EIS has examined existing literature and best practices for managing enterprise privacy risk and has developed a series of recommendations designed to set Oregon on the path to effectively manage and mitigate privacy risk statewide. The primary recommendation is the state should establish a Chief Privacy Officer role dedicated to establishing an Enterprise Privacy Program. This Chief Privacy Officer role is a critical component of building a privacy program and incorporating privacy guidance into EIS' policies and guidelines for state agencies.

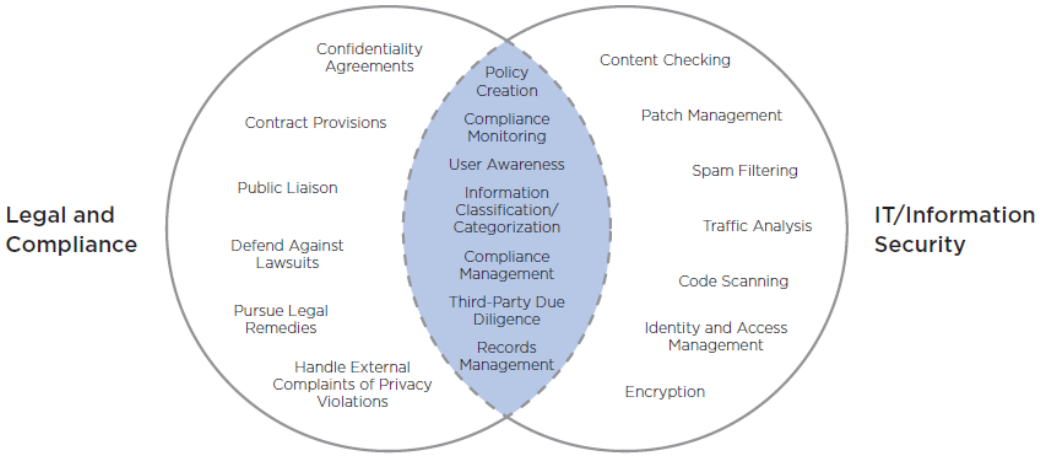
Data Governance, Information Security, Data Privacy: Three Distinct Roles

As a result of the close relationship between data privacy, data governance, and information security, there can be a tendency to conflate the roles and responsibilities of Chief Data Officers, Chief Information Security Officers, and Chief Privacy Officers. While these roles share responsibility for data management and appropriate management of data risk, these three roles are distinct disciplines with distinct responsibilities. Public-sector Chief Data Officers have oversight over data governance, the effective and ethical use of data, data equity, building a data-informed culture, and open data/data transparency. In other words, Chief Data Officers are focused on how we leverage data entrusted to the state as a strategic asset and gain value and insight from our data. Chief Information Security Officers are focused on security operations, administration, architecture, identity, and access management. In effect, Chief Information Security Officers retain responsibility for how we protect and manage access to the state's data assets through technical, physical, and administrative controls. Chief Privacy Officers are primarily focused on the regulatory and legal compliance of how we manage data, specifically the management of risk associated with data collection, storage, management, and sharing. Chief Privacy Officers are responsible for determining and adopting appropriate privacy frameworks, such as the National Institute of Standards and Technology (NIST) Privacy Framework and/or privacy by design, to manage privacy at the enterprise level.

Beyond the privacy/security distinction and differentiation of operational responsibilities between Chief Data Officers, Chief Information Security Officers and Chief Privacy Officers, 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, 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 they hold in trust. In its 2013 report, Gartner explicitly acknowledged the lack of clarity around roles and responsibilities; with privacy activities being shared between legal and information security.[23]

[23] CEB (acquired by Gartner), "Implement an Effective Data Privacy Program."

Figure 2. Privacy Activities Shared Between Legal and Information Security[24]



Source: CEB analysis.

To build an effective program for managing enterprise privacy risk and protection of personally identifiable information, there needs to be a clear delineation between the roles and responsibilities of the Chief Data Officer, Chief Privacy Officer, and Chief Information Security Officer. The responsibilities and expectations of each individual role are distinct, but together they share accountability to manage the privacy and security of data and information created within the state of Oregon. The figure below shows the areas of overlap and separation between the distinct roles of Chief Privacy Officer, Chief Data Officer, and Chief Information Security Officer.

Figure 3. Overlap and Separation between the Chief Data Officer, Chief Information Security Officer, and Chief Privacy Officer

[24] Ibid.

While there are shared activities amongst these three roles to effectively manage and mitigate risk, privacy, data governance and security are not equivalent. It is critical to view privacy as a separate function, focused, first and foremost on personal data; *i.e.*, "why personal data is being collected, what the lawful uses are, how long it can be retained, and who has access to it."[25]

The Chief Privacy Officer: The Necessity of a Distinct Role

EIS has determined the appropriate role for managing enterprise privacy risk is the Chief Privacy Officer, a dedicated executive with central responsibility for managing and mitigating privacy risk, establishing privacy practices, building an enterprise privacy risk assessment, and working with agencies to protect private information and data. The Chief Privacy Officer role is a necessity to ensure appropriate attention and skills are dedicated to managing enterprise privacy, as opposed to incorporating responsibility for enterprise privacy into an existing leadership role within EIS. Stakeholder feedback as part of EIS outreach efforts confirmed EIS' finding that the Chief Privacy Officer role aligns with observed public and private sector best practices as a foundational and critical element in addressing enterprise privacy risk and management. In establishing a privacy program, a threshold issue is ownership of the privacy program—absent clear ownership, there is a substantial risk that privacy initiatives will fail. With lack of a single dedicated executive leader, the state runs the risk of privacy efforts being diffused across multiple roles resulting in loss of energy and resourcing as privacy becomes deprioritized amongst executive leaders' competing priorities. On the individual level, Gartner has identified essential competencies for a privacy leader, including: regulatory expertise, risk management focus, strategic business mind-set and technological know-how.[26]

In terms of educational background and certifications, a NASCIO survey found that among the twelve Chief Privacy Officers surveyed, seven (58%) Chief Privacy Officers had a law degree, eight (67%) were working on an IAPP certification (e.g., Certified Information Privacy Professional), and several others had additional or advanced degrees in public health and education.

In some instances where a Chief Privacy Officer does not exist, privacy responsibility can be delegated to a Chief Data Officer role. The Harvard Business Review, in their article *Are You Asking Too Much of your Chief Data Officer?* notes that incorporating privacy into the Chief Data Officer role sets up the Chief Data Officer for an inability to deliver on the role's primary mandates: "Clearly it would be difficult for one person to perform all of these diverse roles effectively. They require different backgrounds and capabilities."[27] EIS has found that if responsibility for privacy were to remain solely with the Chief Data Officer, an existing executive role within EIS, there would be limited resourcing and capacity available to establish a true enterprise approach to privacy. The Chief Data Officer role is primarily focused on data governance, ethical use of data, open data and transparency, and data literacy, with a tangential relationship to privacy through data ethics and data literacy, as well as managing privacy risk associated with release of open data. While the Chief Data Officer has responsibility for managing data, the Chief Data Officer is not a dedicated role responsible for managing privacy. If privacy were to be incorporated into the Chief Data Officer role, there would still be a need for roles responsible for managing privacy risk within EIS, as the CDO would not be able to manage and build a privacy program without additional staff support to develop and execute the program. The incorporation of enterprise privacy would also represent an increase in scope for the Chief Data Officer role without an addition of the legal expertise common within the Chief Privacy Officer knowledge, skills, and abilities. For these reasons, EIS has determined that it is not feasible to incorporate privacy related duties into the Chief Data Officer role and maintain a focus on enterprise privacy risk management that is appropriate for the scope of the state's needs.

---

[25] McCann, Brendan. "Build a Privacy Program." Info~Tech Research Group, n.d.
[26] CEB (acquired by Gartner). "Implement an Effective Data Privacy Program."
[27] Davenport, Thomas, and Bean, Randy. "Are you Asking too Much of Your Chief Data Officer?" *Harvard Business Review,* February 7, 2020. https://hbr.org/2020/02/are-you-asking-too-much-of-your-chief-data-officer

Similarly, while the Chief Information Security Officer is responsible for securing our systems against unwanted breach or attack, incorporating enterprise privacy risk into the Chief Information Security Officer role would represent similar challenges related to resourcing and expertise. The Chief Information Security Officer would typically work collaboratively with a Chief Privacy Officer to effectively secure systems and establish a Breach Response Plan, but the Chief Information Security Officer remains focused on information and data systems. Were privacy to be incorporated in the Chief Information Security Officer role, EIS would need to identify and establish roles to create and oversee an enterprise privacy program and to provide guidance to state agencies. These responsibilities instead are best suited to a single executive role with a particular focus on privacy. These recommendations are underscored by the Secretary of State's findings in their audit *The State Does Not Have a Privacy Program to Manage Enterprise Data Privacy Risk,* which articulated the need for a single position tasked with managing enterprise data privacy risk for the state and recommended creation of a Chief Privacy Officer role within EIS.[28]

Recommendation: Establish Statutory Authorization and Budgetary Support for a Chief Privacy Officer and Enterprise Privacy Program

Within the public sector, state government in particular, the appointment of a Chief Privacy Officer and establishment of a privacy program implicates issues of statutory authority and budgetary appropriations. In addition to addressing specific resource constraints, enabling legislation provides legitimacy and clarifies statutory authority and obligations relative to Executive Branch agencies—this is particularly important within the context of a decentralized IT operating environment such as Oregon. As part of engagement sessions with stakeholders, EIS asked if there were any potential risks or limitations associated with establishing a Chief Privacy Officer. All stakeholder groups agreed that the primary concern is related to effective budgetary authority and staff resourcing to accomplish the body of work associated with a Chief Privacy Officer. There was concern that creation of an executive role alone was not sufficient to appropriately build, sustain, and maintain a dedicated privacy program with expectations of supporting and providing leadership to all state agencies. This feedback is consistent with EIS's research into best practices and current surveys.

Gartner found that among 334 responding organizations, only 10% of respondents reported there was no dedicated budget allocated to privacy risk and more than 75% of the respondents spent $500,000 or more.[29]

In support of the recommendation that the state establish and provide budgetary authority to a Chief Privacy Officer role, EIS recommends the Legislature establish law to codify the role and responsibilities of a Chief Privacy Officer, set expectations for state agencies in managing their individual agency privacy risk, and clarify an appropriate relationship between the Chief Data Officer and Chief Privacy Officer. By establishing a Chief Privacy Officer role within legislation, the state will be able to effectively articulate the differing roles between data governance, data privacy, and data security, and carve out critical privacy duties belonging to the Chief Privacy Officer.

Recommendation: Privacy Program Deliverables

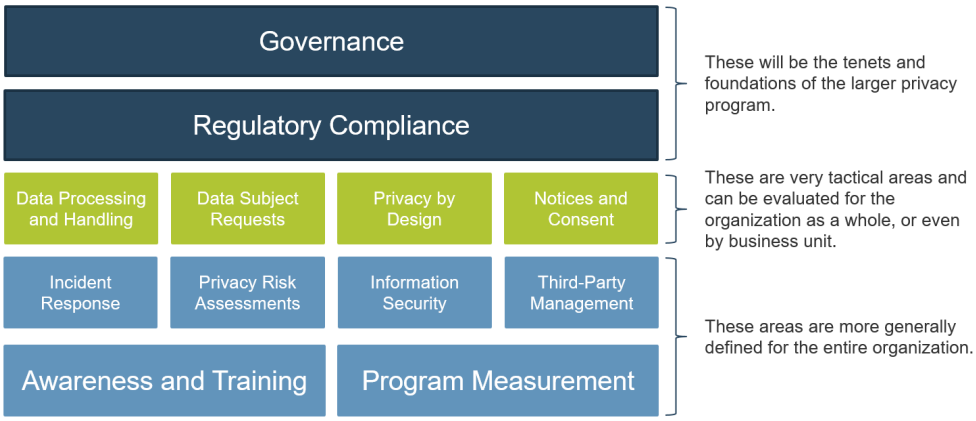
EIS examined best practices from two technology research firms, Info-Tech Research Group and Gartner, to identify critical deliverables associated with an Enterprise Privacy Program and examine possible frameworks for implementation within the state of Oregon government. As part of its "Build a Privacy Program" toolkit, Info-Tech proposes an over-arching Privacy Framework (hereinafter, the "Framework"). The Framework is used to evaluate or assess the current state of privacy leadership and compliance (i.e.,

---

[28] Oregon Secretary of State Audits Division. *The State Does Not Have a Privacy Program to Manage Enterprise Data Privacy Risk*. November 2020. http://records.sos.state.or.us/ORSOSWebDrawer/Recordhtml/7672528
[29] Willemsen, Bart, and Bernard Woo. "Use These Frequently Asked Questions When Starting a Privacy Program." *Gartner*, September 5, 2019.

privacy gap analysis) within an organization and outlines key domains within a privacy program—it is also a useful visual reference.

Figure 4. Info-Tech Privacy Framework[30]



In examining this Framework and the critical components of an Enterprise Privacy Program, EIS recommends the Chief Privacy Officer be tasked with key deliverables associated with evaluating and assessing the state's enterprise privacy landscape. The primary deliverable recommended by EIS is a Privacy Gap Analysis to evaluate and baseline the current state of information and data privacy management within Oregon. This Gap Analysis should be leveraged by the Chief Privacy Officer to determine the needs and guiding principles of additional privacy tools and frameworks, such as the incorporation of a Privacy Impact Assessment or other evaluative framework into IT Projects.

ASSESSMENT; *AKA* PRIVACY GAP ANALYSIS

With an executive leader such as a Chief Privacy Officer in place, Info-Tech recommends conducting a privacy-gap analysis using the Framework to identify gaps and to develop a roadmap of prioritized privacy initiatives. Regardless of whether one employs the Info-Tech methodology or another available privacy framework and methodology, the assessment phase is critical in implementing a privacy program. This need to establish a baseline and enterprise privacy risk assessment and evaluation align with EIS' recommendation to develop and leverage an enterprise risk assessment to give the Chief Privacy Officer an opportunity to establish a baseline for Oregon's privacy maturity and overall risk, as well as develop enterprise guidance that state agencies can leverage to protect private information. This period of assessment and evaluation may lead to further incorporation of tools such as Privacy Impact Assessments for IT projects, or further recommendations based upon the Chief Privacy Officer's findings.

PRIVACY IMPACT/RISK ASSESSMENTS (PIAS)

Privacy risk assessments, aka privacy impact assessments (PIA) and the policies and process governing their application are foundational deliverables within any privacy program—particularly, when it comes to new IT initiatives as post-implementation privacy remediation (bolt-on measures) increasing "system and infrastructure complexity, cost, and meantime privacy risk."[31] As previously noted, the recent Gartner assessment found this capability absent both within CSS and within Executive Branch agencies. Privacy impact assessments are frequently incorporated into privacy programs as an effective measure for gauging

[30] McCann, Brendan. "Build a Privacy Program."
[31] Willemsen, Bart. "Use These Privacy Deliverables in Every IT Development Project," *Gartner* (2018).

the ways new IT projects, data collection streams, or programs impact the data an organization holds as well as identifying and mitigating potential risk before new datasets are collected.

From a compliance perspective, PIAs are explicitly required by a growing number of jurisdictions and compliance regimes (e.g., GDPR, Ohio, British Columbia, the federal government under the E-Government Act of 2002 et al.). Furthermore, according to Gartner, the formalization of rules governing the privacy impact assessment process represent one of four steps necessary to establish an effective data privacy program.[32] Privacy Impact Assessments better enable effective data planning and lifecycle management strategies at the outset of new IT projects and will also support critical transparency by design requirements established for new technology initiatives within ORS 276A.365, "Information Management by State Agencies," requiring state agencies consider system scalability and flexibility and data structures as part of any new IT planning processes or procurements. The PIA process allows time for an agency to perform due diligence in the development of new data collections and includes thoughtful planning activities to ensure a state agency addresses privacy at the outset of a new program or initiative.

To effectively implement the stages within the Privacy Impact Assessment, the state of Oregon must undertake foundational privacy risk assessment and mitigation strategies. The PIA is a marker of a mature Enterprise Privacy Program, and requires the development of staff knowledge, skills and abilities through dedicated privacy related outreach and training in advance of implementation. Incorporation of a Privacy Impact Assessment into existing oversight models within EIS, such as StageGate, would require further investment in Oversight Analyst staff and additional privacy roles within EIS to effectively govern and provide feedback on submitted PIAs.

Absent a current executive leader for managing privacy risk and the lack of any existing gap analyses or evaluations on the state's current privacy landscape, EIS recommends tasking the Chief Privacy Officer with utilizing findings from the Privacy Gap Analysis to identify the appropriate approach(es) for the state of Oregon in conducting Privacy Impact Assessments for IT Projects or technology procurements. While the Privacy Impact Assessment is considered a foundational aspect of any enterprise privacy program, there first exists a need for an evaluation and baselining phase in the creation of an enterprise privacy approach before EIS makes recommendations for specific tools or frameworks to be adopted. Additionally, the development of a Privacy Impact Assessment approach for the state should include time spent in discussion with constituents, end-users, and stakeholders within the state of Oregon in advance of being launched as a state requirement. The need for stakeholder engagement further underscores the value of privacy related outreach and engagement with stakeholders and the community, and the need for a deliberate and diligent approach before making firm recommendations on how Oregon should approach a PIA process.

Recommendation: Develop Privacy Outreach, Education and Engagement Strategies

Protecting and managing privacy is about maintaining public trust and ensuring that when private data is entrusted to the state of Oregon, it is appropriately managed and secured. A critical component of managing privacy risk involves investing in education, outreach, and engagement with the individuals whose data is held in trust by the state of Oregon. As the data streams collected by the state become increasingly diverse and complex, there is a critical need to "preserve the privacy, quality, and integrity of the data we hold in trust," as identified within Oregon's Data Strategy.[33] Additionally, as consumer related privacy matters become more mainstream, government must continue to have respect for the self-determination of its constituents in understanding how their data is collected, shared, and utilized within state systems. EIS is aware that user outreach and engagement are critical components of both an Enterprise Privacy Program and an Enterprise Data Program and recommends the Chief Privacy Officer and Chief Data Officer work together collaboratively on a stakeholder engagement and outreach approach that educates constituents about

[32] CEB (acquired by Gartner), "Implement an Effective Data Privacy Program."
[33] Enterprise Information Services. *Oregon's Data Strategy: Unlocking Oregon's Potential*. February 2021. https://www.oregon.gov/das/OSCIO/Documents/68230_DAS_EIS_DataStrategy_2021_v2.pdf

privacy, data as a strategic asset, use of data within state systems, open data, and fundamental privacy practices or rights as established.

Enterprise privacy approaches seek to appropriately respect the rights of individuals and groups to have their privacy preserved and maintained within the complex technology systems of the state. The development of privacy principles and similar "bill of rights" practices related to privacy, such as the Fair Information Practices[34], or the Organization for Economic Co-operation and Development (OECD) Privacy Guidelines[35], identify the need for regular outreach and education to facilitate individual participation and self-determination. In 2021, EIS recognized the growth of these privacy principles and practices within government and conducted a comparative analysis of the privacy principles of Portland, Oakland and Seattle. Through this study, three core themes emerged in the development of government privacy principles: transparency, accountability, and data protection.[36] These three themes touch on the intersections of open data, transparency, and privacy within the state of Oregon and encapsulate the need for both the Chief Data Officer, as the role responsible for open data and transparency, and the Chief Privacy Officer, responsible for data privacy, to work closely in the development of any privacy principles or practices for the state. Collaboration between the Chief Data Officer and the Chief Privacy Officer creates opportunities for the state of Oregon to identify principles and practices related to data ethics and privacy that ensure the rights of Oregonians are respected within state data systems. As the Chief Privacy Officer begins to build an Enterprise Privacy Program, there should be consideration paid to the adoption or creation of privacy principles for the state of Oregon, including space for stakeholder engagement and community feedback in their development.

One possible model for constituent engagement within Oregon related to privacy can be observed from the City of Portland's dedicated outreach strategy for Portland's Surveillance Technologies Policy.[37] As part of the policy development process, the City performed dedicated community outreach and education events to first define what surveillance technologies are, how they collect and utilize information, and how Portland residents are impacted by surveillance technologies. Portland invested in foundational education and outreach to appropriately educate and increase awareness of the merits and drawbacks of surveillance technologies in advance of engaging Portlanders in helping to draft and provide policy feedback. As part of Oregon's approach, the Chief Data Officer should first establish baseline data literacy outreach and training for constituents and community members, in how the state collects and utilizes data, and provide education in open data and transparency to increase access to publicly available state data resources. By setting the stage for the state's data ecosystem, Oregon enables the Chief Privacy Officer to engage with an informed and resourced populace on matters related to information privacy and security.

As Oregon establishes and develops an Enterprise Privacy Program, constituent and stakeholder involvement and education will be central in supporting Oregon's approach to ethical privacy risk management. EIS recommends the Chief Privacy Officer be responsible for developing community outreach and engagement strategies as well as collaborating with the Chief Data Officer to ensure Oregonians receive valuable data literacy education so our constituencies can fully engage with the state of Oregon in the development of an Enterprise Privacy Program.

---

[34] International Association of Privacy Professionals (IAPP). *Fair Information Practice Principles.* https://iapp.org/resources/article/fair-information-practices/

[35] Organization for Economic Co-operation and Development (OECD). *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, "The Privacy Guidelines"*. 2013. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

[36] Enterprise Information Services. *An Analysis of the privacy Principles Implemented by the Cities of Portland, Seattle, and Oakland.* May 2021. Internal Report, unpublished.

[37] City of Portland. "Help us Build the City's Surveillance Technologies Policy!" February 22, 2022. https://www.smartcitypdx.com/news/2022/2/22/help-us-build-the-citys-surveillance-technologies-policy

Summary

EIS has closely examined the merits of establishing and appointing a dedicated role responsible for information protection and privacy guidance for state agencies, in addition to analyzing the merits associated with establishing a program for managing enterprise privacy risk within Oregon. Current best practices and leading thought is that privacy is best managed through a dedicated executive role such as a Chief Privacy Officer, but the existence of a Chief Privacy Officer does not guarantee effective privacy management absent investment of statutory authority and budget to mature privacy approaches within state agencies. The recommendations presented within this report are designed to articulate not only the value of the Chief Privacy Officer role as a separate responsibility from that of a Chief Data Officer, Chief Information Security Officer, or other EIS executive role, but to underscore the necessity of appropriate staffing and education to adopt and embed privacy risk management into each Executive Branch agency.

In considering creation of a Chief Privacy Officer role within the state of Oregon, EIS and the Legislature should work collaboratively to ensure that appropriate statutory authority, resourcing, and budget are provided to set the Chief Privacy Officer up for successful delivery of program outcomes. Similarly, the Chief Privacy Officer should be afforded an appropriate length of time to undertake a thorough evaluation of the state's current privacy approaches and to assess enterprise privacy risk, in advance of making formal recommendations related to privacy program structures or in the development and incorporation of a Privacy Impact Assessment or similar tool for EIS oversighted IT projects.

Lastly, data privacy management should be a collaborative process between the state and its constituents. This requires dedicated time and energy spent in developing community engagement strategies, communication plans, and in resourcing both the Chief Privacy Officer and Chief Data Officer to perform stakeholder engagement, outreach and training related to data and privacy concerns. Given the rapidly evolving and increasingly complex privacy regulatory environment, coupled with increasing public concern over the collection, protection, use, and dissemination of citizen data, privacy program development should afford sufficient time for public comment and feedback as a foundational action before moving into implementation.

Sources Cited

"Information Security Management Capabilities Model, Observations and Recommendations." Gartner, February 10, 2020.

"What Is Privacy." International Association of Privacy Professionals. Accessed March 9, 2020. https://iapp.org/about/what-is-privacy/.

City of Portland. "Help us Build the City's Surveillance Technologies Policy!" February 22, 2022. https://www.smartcitypdx.com/news/2022/2/22/help-us-build-the-citys-surveillance-technologies-policy

Corporate Executive Board (CEB, Gartner. "Implement an Effective Data Privacy Program." In Information Security in a Box: A Guide for Establishing Baseline Maturity, 2013 (updated January 2020).

Davenport, Thomas, and Bean, Randy. "Are you Asking too Much of Your Chief Data Officer?" Harvard Business Review, February 7, 2020. https://hbr.org/2020/02/are-you-asking-too-much-of-your-chief-data-officer

Enterprise Information Services. An Analysis of the privacy Principles Implemented by the Cities of Portland, Seattle, and Oakland. May 2021. Internal Report, unpublished.

Enterprise Information Services. An Analysis of the privacy Principles Implemented by the Cities of Portland, Seattle, and Oakland. May 2021. Internal Report, unpublished.

Enterprise Information Services. Oregon's Data Strategy: Unlocking Oregon's Potential. February 2021. https://www.oregon.gov/das/OSCIO/Documents/68230_DAS_EIS_DataStrategy_2021_v2.pdf

Glasscock, Amy Hille. "Perspectives on Privacy: A Survey and Snapshot of the Growing State Chief Privacy Officer Role." NASCIO, March 27, 2019. https://www.nascio.org/resource-center/resources/perspectives-on-privacy-a-survey-and-snapshot-of-the-growing-state-chief-privacy-officer-role/.

Glasscock, Amy Hille. "Privacy Progressing: How the State Chief Privacy Officer Role is Growing and Evolving." NASCIO, June 15, 2022. https://www.nascio.org/resource-center/resources/privacy-progressing-how-the-state-chief-privacy-officer-role-is-growing-and-evolving/

Henein, Nader, and Bart Willemsen. "The Privacy Officer's First 100 Days." Gartner, April 15, 2019.

Henein, Nader, and Willemsen Bart. "The State of Privacy and Personal Data Protection, 2019-2020." Gartner, April 15, 2019.

Henein, Nader, Woo, Bernard, and Willemsen Bart. "State of Privacy – Regional Overview Across North America." Gartner, February 4, 2022.

International Association of Privacy Professionals (IAPP). Fair Information Practice Principles. https://iapp.org/resources/article/fair-information-practices/

McCann, Brendan. "Build a Privacy Program." Info~Tech Research Group, n.d.

O'Brien, Danny. "Data Privacy or Data Protection Day? It's a Human Right, Either Way." Electronic Frontier Foundation, January 29, 2020. https://www.eff.org/deeplinks/2020/01/data-privacy-or-data-protection-day-its-human-right-either-way.

Oregon Secretary of State Audits Division. The State Does Not Have a Privacy Program to Manage Enterprise Data Privacy Risk. November 2020. http://records.sos.state.or.us/ORSOSWebDrawer/Recordhtml/7672528

Organization for Economic Co-operation and Development (OECD). Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, "The Privacy Guidelines". 2013. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188

Willemsen, Bart, and Bernard Woo. "Use These Frequently Asked Questions When Starting a Privacy Program." Gartner, September 5, 2019.

Willemsen, Bart, and Nader Henein. "Predicts 2020: Embrace Privacy and Overcome Digital Ambiguity to Drive Digital Transformation." Gartner, November 14, 2019.

Willemsen, Bart. "Hype Cycle for Privacy, 2019." Gartner, July 11, 2019.

Willemsen, Bart. Use These Privacy Deliverables in Every IT Development Project (2018).