Secretary of State
Oregon Audits Division

Department of Administrative Services and Enterprise Information Services

The State Does Not Have A Privacy Program to Manage Enterprise Data Privacy Risk

November 2020
Report 2020-37

Secretary of State Bev Clarno
Audits Division Director Kip Memmott

Secretary of State
Oregon Audits Division

Executive Summary

Department of Administrative Services, Enterprise Information Services

The State Does Not Have A Privacy Program to Manage Enterprise Data Privacy Risk

Why This Audit is Important

» Growth in information technology has made it easier to collect personally identifiable information (PII), which puts that information at increased risk of being compromised.

» State agencies collect PII on virtually all Oregonians, including health and vital records, driving records, education data, and tax information.

» The federal government lacks a current and comprehensive privacy law, leaving states to pursue legislation to ensure data privacy is adequately addressed.

» Across 17 sectors, the public sector takes the second longest to detect and contain a data breach. Longer response times result in increased exposure of compromised data.

» In 2017, Oregon enacted House Bill 3361, which established open data and data governance requirements, including some tasks related to information privacy.

What We Found

1. Oregon does not have a statewide official responsible or accountable for managing data privacy risk. (pg. 7)

2. Enterprise Information Services (EIS) has not provided agencies with clear guidance on how to respond to a security incident involving PII. (pg. 10)

3. Though still developing foundational policy and strategy, the Chief Data Officer has made progress in implementing enterprise data governance requirements. (pg. 12)

What We Recommend

Our report includes one recommendation to EIS. Although COVID-19 has negatively affected the state budget, we recommend EIS request funding to establish a statewide privacy office and appoint a senior official responsible for managing an enterprise privacy program. Additionally, EIS should clarify roles and provide training to ensure agency personnel understand their role in responding to incidents involving PII.

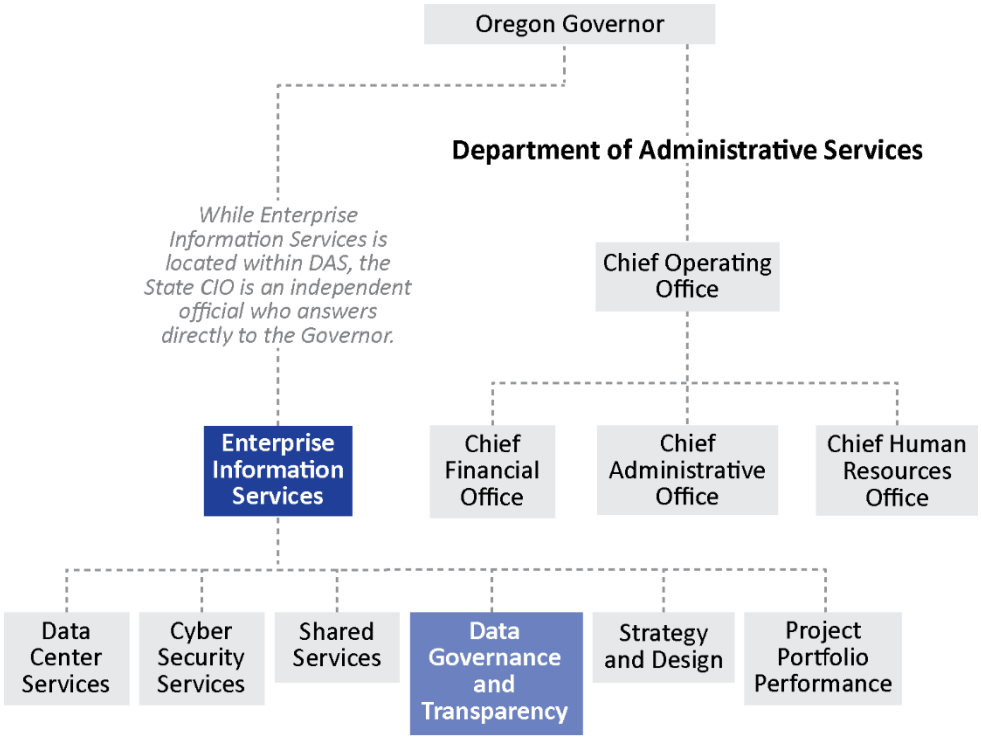
EIS agreed with our recommendation. Their response can be found at the end of the report.

Introduction

Oregon state agencies, boards, and commissions collect and store tremendous amounts of personally identifiable information (PII) as part of their various business processes. People provide their personal information to state agencies for a variety of reasons, such as licensing, financial assistance, and social services. Providing these services often requires state agencies to maintain PII related to protected health information, criminal history records, driving records, tax information, and various licensing data, to name a few. Entities that collect PII should ensure the privacy and protection of such data.

Enterprise Information Services (EIS) maintains statewide information technology (IT) policy and oversight. The office's responsibilities include oversight of IT security for executive branch state agencies. In 2017, the Legislature approved funding for the Chief Data Officer (CDO), which also resides within EIS.

The purpose of this audit was to assess whether Oregon has a governance structure in place to manage the risks to data privacy for the PII it collects. As part of this effort, we assessed the status of the CDO's progress in implementing privacy-related requirements set forth by the Legislature in 2017.



Data privacy is a complex topic

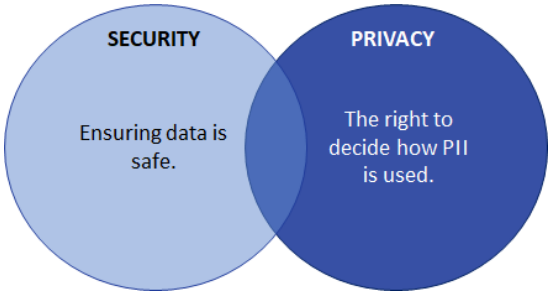
While most people agree that data privacy is important, the concept of data privacy is difficult to succinctly describe. The International Association of Privacy Professionals (IAPP) does not provide a definition of privacy, but notes that it is a nebulous concept which means different things to different people.[1] We identified the following definitions of privacy from other sources:

[1] The IAPP is a not-for-profit professional community and resource committed to providing a forum for privacy professionals to share best practices, track trends, advance privacy management issues, standardize the designations for privacy professionals, and provide education and guidance on opportunities in the field of information privacy.

- "The right to be left alone and to keep certain matters secluded from public view." - Oxford Dictionary of Law;
- "The right of a party to maintain control over and confidentiality of information about itself." – National Institute of Standards and Technology; and
- "The rights of an individual to trust that others will appropriately and respectfully use, store, share, and dispose of his/her associated personal and sensitive information in accordance for the purposes for which it was collected or derived ... and to reasonably control and be aware of the collection, use, and disclosure of associated personal and sensitive information." – ISACA[2]

These definitions encompass two main elements: the right of individuals to decide how their personal information is used and the right to have their information remain safe. The first focuses primarily on privacy, while the latter focuses on security, complicating the task of untangling data privacy from information security. In general, privacy programs are responsible for managing risks to individuals associated with processing PII, while security programs are responsible for ensuring the confidentiality, integrity, and availability of information.

Figure 1: Security and privacy are distinct but intersecting concepts



Although security is an important consideration for an effective privacy program, privacy risk management must also address factors such as compliance with privacy laws and mechanisms to communicate data processing options and preferences. Similarly, security programs must strive to protect information beyond PII, such as ensuring the integrity of state financial records or the availability of information systems through which public services are provided. While these two concepts are each important and complex unto themselves, they are also closely intertwined, in that the security of PII is an integral element of an effective privacy program.

For the purpose of this audit, we define PII as the information that can be used to identify an individual. While definitions vary, PII generally includes social security numbers, date and place of birth, or a person's full name. Additionally, data that is not considered PII, such as a person's employer, can become PII when combined with other identifying information, such as date and place of birth. However, not all PII is created equal; some is more sensitive and could result in greater harm if disclosed. For example, an individual's social security number is more sensitive than their zip code. Safeguards should be considered based on the sensitivity of the information.

Individuals and organizations both have a stake in data privacy

Human beings value their privacy. However, state agencies often require PII in order to provide services. When people interact with the online forms and agency computer systems that collect PII, they may not realize the potential risks to their privacy as they interact with those systems. Moreover, this risk may not be fully recognized by the organizations that collect the information.

[2] ISACA is a global professional community that strives to inspire and enable innovation through technology by researching and developing solutions, best practices, and frameworks, as well as offering professional certifications and facilitating community collaboration.

As the growth in IT has made it easier to collect, maintain, and store data about an individual, incidents of data loss and unauthorized use of data have also grown in both the public and private sectors. Such incidents can lead to identity theft or fraudulent activity that may result in inconvenience, embarrassment, financial loss, or other harm for the individual. Beyond the threat of identity theft or fraud, inappropriate access to personal information may lead to social issues such as unequal bargaining position, discrimination, and encroachment on moral freedom and human dignity.

Privacy risk
The risk to individuals that a disclosure of their private information could result in personal or financial harm, discrimination, and encroachment.

State agencies also face consequences if data privacy is not adequately managed. Failure to maintain compliance with federal regulations can result in financial penalties. Additionally, agencies who fail to adequately ensure individual privacy may face a loss of public trust and potential litigation from individuals whose information is compromised.

Data breaches are inevitable — it is not a matter of if, but when, a breach will occur. While the severity of a breach may vary, private companies, such as Equifax and Target, have made headlines over breaches that affected millions of customers. Government entities have also been affected. In 2019, the Texas Health and Human Services Commission was fined $1.6 million when a data breach made the personal health information of 6,617 people available online. In 2020, Oregon was one of 28 states involved in a multi-state settlement agreement with Tennessee-based Community Health Services, Inc., following a 2014 data breach which copied and transferred data from approximately 6.1 million patients, including names, birthdates, addresses, and social security numbers.

Similar breaches have occurred in Oregon. In 2014, the personal information of more than 851,300 people was compromised after a breach at the Oregon Employment Department. In 2019, the Oregon Health Authority notified the public that a breach compromised the protected health information of patients at the Oregon State Hospital. Not all breaches threaten PII or individual privacy; however, Oregon must be diligent in its efforts to mitigate the risk of data breaches, especially those involving the PII of Oregonians.

Data privacy laws and regulations are evolving

A major component of mitigating privacy risk is ensuring compliance with privacy laws and regulations. As technology advances, laws are created or amended to address new threats and vulnerabilities. It is critical for entities that collect PII to understand the ever-evolving data privacy landscape and to implement effective tools and processes to ensure compliance with current legal requirements.

Data privacy laws have spread globally since originating at the national level over a century ago. Privacy laws now exist in places throughout the world, but vary in form by country and region. Of significance is the General Data Protection Regulation (GDPR), enacted by the European Union in 2016. The GDPR establishes privacy standards for any organization, including government bodies, that targets or collects data

Figure 2: GDPR establishes certain rights for data subjects in the European Union

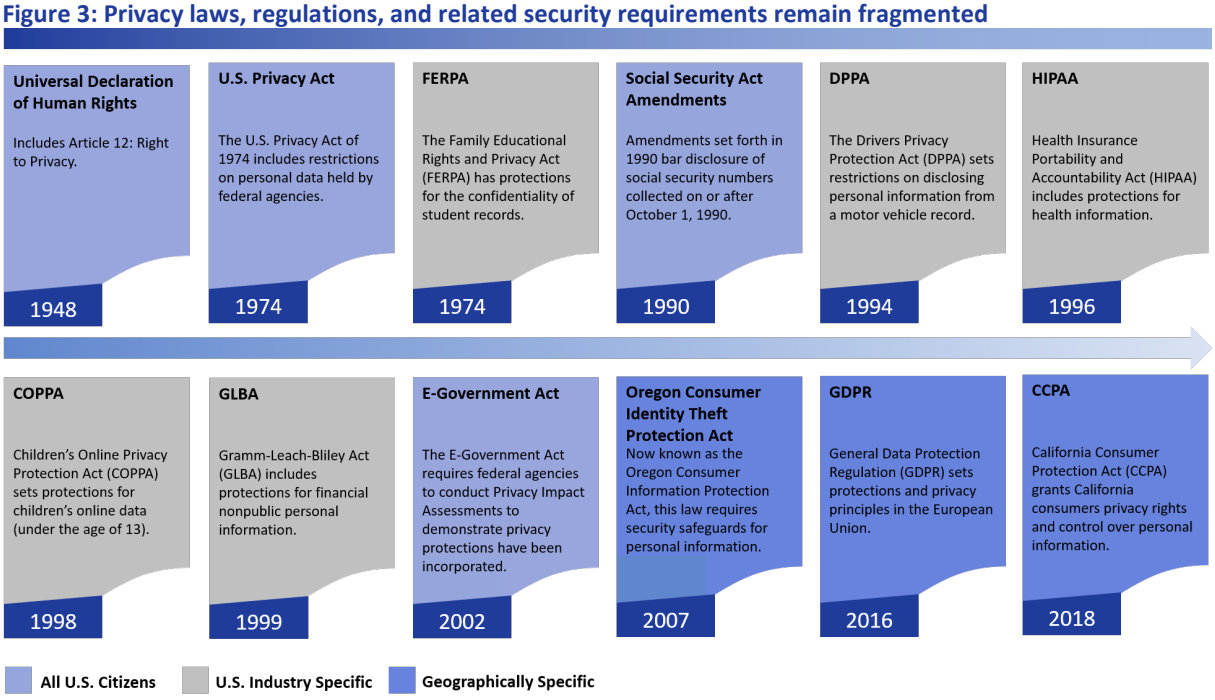
related to people in the European Union and levies fines for those who violate those standards. GDPR sets forth principles related to the processing of personal data and the rights for individuals. This legislation has invigorated discussions on privacy legislation in the United States and globally.

States have begun to address gaps in federal privacy law

At a federal level, the U.S. lacks a current and comprehensive privacy law. The Privacy Act of 1974 establishes fair information practices for personal information collected and maintained in information systems by federal agencies. However, an overview of the Act issued by the U.S. Department of Justice Office of Privacy and Civil Liberties in 2015 stated that "the Act's imprecise language, limited legislative history, and somewhat outdated regulatory guidelines have rendered it a difficult statute to decipher and apply."[3]

In the five years since the U.S. Department of Justice's review of the federal Privacy Act, there has been little traction at the federal level to implement a comprehensive approach to address privacy, despite the introduction of several bills aimed at doing so. Though a comprehensive federal approach is lacking, several regulations set forth requirements to protect personal information relevant to specific industries, such as student records and protected health information. See Figure 3 for some of the relevant laws and regulations.

Figure 3: Privacy laws, regulations, and related security requirements remain fragmented



In lieu of a comprehensive federal approach, government leaders around the nation are pursuing privacy legislation at the state level. However, until recently, these bills have been narrowly scoped, addressing privacy issues in specific sectors.

Recently, states have begun introducing more comprehensive privacy legislation. In 2018, the California Consumer Privacy Act was passed as a landmark bill that provides an overarching approach to privacy and strong privacy protections for California consumers. Since that time, several other states have introduced comprehensive privacy legislation, though some states have struggled to enact these bills into law. This decentralized approach to privacy may lead to a

[3] Download the Overview of the Privacy Act at https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition.

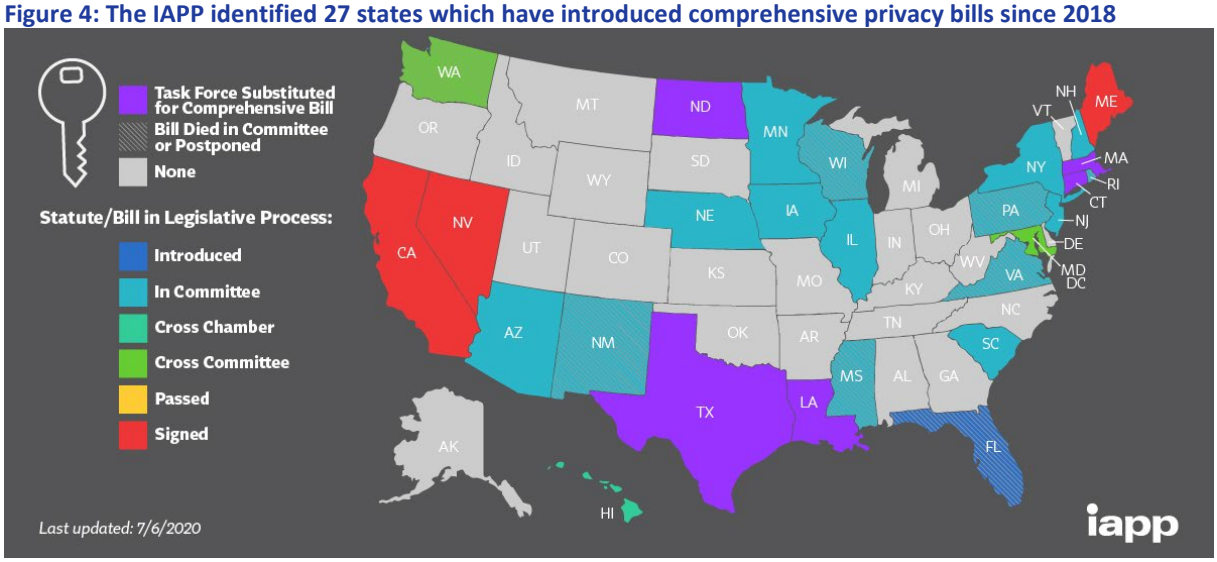
heavy burden on affected organizations and confusing or conflicting information on what rights individuals possess.

Oregon lacks a comprehensive privacy law

Privacy is such an important topic that some states have explicit privacy protections written into their constitutions; Oregon is not one of them. Moreover, as portrayed in Figure 4, comprehensive privacy legislation has not been introduced in the state, although various bills have been introduced to address targeted privacy considerations.

For example, in 2019, Senate Bill 684 established requirements for certain entities which possess personal information to notify consumers of a breach of security. House Bill 2866, also introduced in the 2019 session, would have required entities collecting data to provide clear disclosures and receive express consent from individuals about what they were collecting and how it would be used; however, the bill did not make it out of committee.

Figure 4: The IAPP identified 27 states which have introduced comprehensive privacy bills since 2018



Source: IAPP US State Comprehensive Privacy Law Comparison.

In 2019, Oregon's Attorney General convened a Consumer Privacy Task Force to discuss developments in privacy legislation and consider policy solutions for Oregon. The Attorney General's Office has begun to draft a legislative concept relating to consumer privacy rights and establishing requirements for entities that do business with Oregonians.

EIS is responsible for IT oversight in Oregon

Oregon does not have a department or senior agency official charged with managing privacy risk at the state. However, the State Chief Information Officer is responsible for implementing and maintaining IT governance for state executive department agencies and heads EIS, an organizational division of the Department of Administrative Services.

The State Chief Information Officer and EIS responsibilities include, among other things, adopting rules, policies, and standards for operating IT; making recommendations to the Governor and Legislature concerning IT budget requests; adopting information security plans, rules, policies, and standards; and developing and promoting IT training programs. EIS functions within the state's hybrid model of IT management, wherein EIS provides policy and oversight while agencies are responsible for designing and delivering information systems.

While EIS is organizationally positioned within the Department of Administrative Services, the State Chief Information Officer reports directly to the Governor, rather than to the agency director. EIS is funded primarily through an assessment of state agencies based on the number of positions. In the 2019-21 biennium, EIS had a total approved budget of $80 million and included 118 positions. EIS is comprised of six programs: Project Portfolio Performance, Shared Services, Data Center Services, Cyber Security Services, Strategy and Design, and Data Governance and Transparency.

Data Governance and Transparency is led by the CDO, a position created by the Legislature in 2017 with the passage of House Bill 3361. The CDO was charged with specific tasks related to enterprise data governance and open data, including maintaining a central web portal, developing technical standards for publishing data through the web portal, and establishing an enterprise data and information strategy. Our audit assessed the CDO's status on implementing certain elements of the bill related to data governance and privacy.

Audit Results

While essential to the delivery of services by state agencies, the increasing use of technology magnifies the potential harm to an individual's privacy. Agencies use technology to collect, maintain, use, disseminate, and dispose of sensitive information for virtually all Oregonians. However, the state has not developed an organizational infrastructure to ensure that privacy risks are identified and managed throughout the enterprise, including processes to ensure incidents involving PII are appropriately handled. Without appropriate management throughout the entire data lifecycle, PII could be lost or inappropriately disclosed, putting people at an increased risk for identity theft or other harm.

Oregon does not have a statewide program to manage data privacy risk

State agencies electronically collect and store Oregonians' personal information, such as protected health information, personal income tax data, driving records, criminal history information, and education data. The state has an ethical responsibility to its citizens to understand and address the privacy implications associated with the data it collects. Moreover, many agencies are required to comply with federal regulations governing data privacy and may be required to comply with one or more of an evolving array of privacy laws.

Despite this, Oregon does not have a statewide program to assess and manage data privacy risk. While some statewide officials have responsibilities that intersect with privacy risk management, there is no enterprise program to ensure sensitive personal data collected by agencies is kept private and protected and that privacy rights are communicated by all agencies that collect such information.

Even without a statewide privacy program, state agencies need to address and manage their privacy risks to comply with laws and federal regulations such as HIPAA and FERPA.[4] To this end, many agencies have developed roles and processes to comply with federal privacy requirements. However, this fragmented approach across the enterprise falls short of ensuring that PII held by the state is appropriately managed.

Foundational activities for effective privacy risk management include understanding the organization's risk tolerance, conducting a privacy risk assessment, and establishing privacy values and policies to respond to identified risks. Privacy considerations should be embedded into the entire data lifecycle, as noted in Figure 5, from before the data is collected until it is ultimately destroyed. This requires identifying PII that is accessed or held by the organization as well as third parties. Organizations should develop and implement a governance structure to enable an ongoing understanding of their risk management priorities. This structure should include a senior official with the authority, mission, and resources to manage privacy risk.

Figure 5: The data lifecycle shows how data moves through an organization

[4] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the U.S. Department of Health and Human Services to issue privacy regulations governing individually identifiable health information. The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records.

As state agencies in Oregon collect more citizen data, it is not only pertinent to institute a privacy framework and program, but also to have someone who understands and can interpret laws and regulations to help manage the potential privacy risks. However, Oregon does not have a program or senior official accountable for managing statewide privacy risk. While some statewide officials have responsibilities that relate to privacy risk management, they are not tasked with assessing data privacy risk or implementing processes to mitigate those risks.

The federal government and some other states have privacy officials

Senior privacy officials have been in place at the federal level for over a decade, though the role continues to evolve. Executive branch federal agencies have been required to designate a senior official responsible for information privacy since 2005; however, in 2016, policies on the role and designation of the senior privacy official were revised. Federal agencies are required to appoint a senior official with the expertise and authority to lead and direct the agency's privacy program and carry out privacy-related functions. This official is responsible for leading and directing federal agency privacy programs, including developing privacy policy, overseeing privacy compliance efforts, and managing privacy risks associated with activities that involve PII throughout the data lifecycle.

While the nation's first state chief privacy officer (CPO) was not hired until 2003 in West Virginia, the role has recently gained momentum, with at least 12 states having a CPO or similar position as of 2019. State governments often task the CPO with managing legal risk, ensuring compliance with privacy laws such as HIPAA and FERPA, and creating standards and policies around data privacy risk and compliance. As such, those filling the roles of CPO often have backgrounds in law, policy, government administration, privacy, security, or technology. Law degrees are common among state CPOs, though they typically sit within the state technology office.

As the role of the state CPO develops, states have taken different approaches to data privacy governance. While some states continue to take a decentralized approach to managing privacy, others have begun to develop a more centralized structure. For example, states such as Kentucky, Maryland, and New Jersey have developed enterprise policies and procedures for privacy risk assessments, data protection requirements, and individuals' privacy rights.

The lack of a statewide privacy program exposes the state to several risks

EIS management has acknowledged the need for a senior privacy official at the statewide level. To this end, they have begun to draft a legislative concept for the 2021 legislative session to create a privacy office and appoint a statewide Chief Privacy Officer. However, with budget cuts anticipated in the 2021 legislative session in the wake of COVID-19, this funding may not be available.

Because no individual is tasked with privacy risk at the statewide level, the state has not performed a privacy risk assessment to identify the risks to individuals that occur as a result of the state's collection of PII. Risk assessments are a critical step that help organizations understand how their information systems and processes may create privacy risks for individuals.[5] Once risks are understood, the state can develop policies and procedures to respond to those risks.

---

[5] The NIST Privacy Framework provides that a privacy risk assessment consists of identifying problematic data actions and determining risk based on the likelihood and impact of those actions. NIST emphasizes that impact determination should consider the problems that may be created for individuals as well as the organization.

Since the state has not established a privacy program, there is little guidance articulating the safeguards agencies should have in place to ensure the protection and proper handling of PII. This does not mean the state lacks any protections at an enterprise level. EIS provides guidance and resources to support agencies in protecting their data when it is stored and transmitted. Additionally, it has published an information security policy, plan, and standards to provide direction for the security of information under the state's control. However, this guidance does not include information on what additional precautions should be in place to identify and ensure the privacy and protection of the PII they collect. For example, additional safeguards may be appropriate to control user access to PII, media sanitization when media contains PII, or encryption techniques for devices storing PII.[6]

One gap identified during the audit is that there is some ambiguity regarding the definition of PII in the state. While the Statewide Information Security Plan refers to the Oregon Consumer Information Protection Act for the definition of PII for the state, other state statutes provide different (though similar) definitions for PII.[7]

PII is collected by many agencies, but not clearly defined

Oregon's statewide policies and legislation do not provide a universal definition of PII. In addition to the definition of personal information set forth in the Oregon Consumer Information Protection Act, we identified the following definitions of personally identifiable information in Oregon statute:

- Chapter 192 (Records; Public Reports and Meetings): Personally identifiable information means all information relating to a person that acquires or uses a transit pass or other fare payment medium in connection with an electronic fare collection system, including but not limited to: (i) Customer account information, date of birth, telephone number, physical address, electronic mail address, credit or debit card information, bank account information, Social Security or taxpayer identification number or other identification number, transit pass or fare payment medium balances or history, or similar personal information; or (ii) Travel dates, travel times, frequency of use, travel locations, service types or vehicle use, or similar travel information.
- Chapter 319 (Motor Vehicle and Aircraft Fuel Taxes): Personally identifiable information means any information that identifies or describes a person, including, but not limited to, the person's travel pattern data, per-mile road usage charge account number, address, telephone number, electronic mail address, driver license or identification card number, registration plate number, photograph, recorded images, bank account information and credit card number.
- Chapter 339 (School Attendance; Admission; Discipline; Safety): Personally identifiable information means any information that would permit the identification of a person who reports information using the tip line, and is not limited to name, phone number, physical address, electronic mail address, race, gender, sexual orientation, disability designation, religious affiliation, national origin, ethnicity, school of attendance, city, county or any geographic identifier included in information conveyed through the tip line, or information identifying the machine or device used by the person in making a report using the tip line.
- Chapter 352 (Public Universities): As used in this section, "personally identifiable information" means a student's Social Security number and gender or a student's Social Security number and date of birth.
- Chapter 432 (Vital Statistics): Personally identifiable information means information that can be used to distinguish or trace an individual's identity or, when combined with other personal or identifying information, is linked or linkable to a specific individual.

We sent a survey to 20 judgmentally selected state agencies, boards, and commissions to gain an understanding of the staffing, policies, and procedures in place to address data privacy at the agency level. Of those that responded to the audit survey, 100% of them collect and store PII

[6] Media sanitization is the process to remove information from physical devices such that information recovery is not possible. Encryption is the process that transforms usable data into an unreadable form.
[7] See Appendix A for the definition of personal information provided in the Oregon Consumer Information Protection Act.

from Oregonians. However, without statewide consensus on what data constitutes PII, agencies may not identify all data that is considered PII, particularly when established by statutes that generally apply to programs at other agencies. Moreover, there is increased risk that agencies may be unaware of laws and regulations that dictate how they handle such data.

If agencies do not know they possess PII, there is a risk that they will not have appropriate safeguards in place to protect the data. These controls are necessary to ensure that PII is not inappropriately disclosed, which may cause reputational or financial harm to individuals as a result of identity theft or fraud.

Statewide policies and procedures do not address requirements for providing individuals with notice about how PII is used or their choice in how it may be used, although some agencies may have individual policies that address these requirements. Organizations should provide individuals with information regarding its activities that impact privacy, what choices individuals have regarding how the organization uses PII, and individuals' ability to access and have this information amended or corrected. Effective notice provides individuals with an understanding of how their data will be used and allows them to make informed decisions prior to providing PII to the state.

EIS has not provided agencies with clear guidance on how to respond to a security incident involving PII

A key function of an effective privacy program is the ability to manage cybersecurity events that affect data privacy. This is critical because, as private information flows through the data lifecycle, each transaction increases the risk for data corruption, error, or leakage. In addition to the potential costs to organizations, these incidents can result in reputational, emotional, or financial harm for individuals, and in some cases, risks to physical safety.

The state lacks enterprise policies and procedures for how to respond to incidents where PII has been compromised

The state does not have comprehensive guidance on how to respond to security incidents involving PII. While statewide security incident response policies, procedures, standards, and plans touch on some elements of what an agency should consider when responding to a security incident involving PII, they do not address the risks specifically associated with a potential breach of PII.

An **information security event** is an observable, measurable occurrence in respect to an information asset that is a deviation from normal processes.

An **incident** is a single or series of unwanted or unexpected information security events that result in harm or pose a significant threat of harm to information assets.

Leading practices state that organizations should develop an incident response plan for incidents involving PII, which informs policies and procedures on how to handle such incidents. Policies covering how to handle incidents involving PII should be developed in addition to general incident response policies, as these events are different from regular incidents and may require additional actions. Security and privacy standards suggest that the privacy incident response plan should be developed under the leadership of a senior official responsible for maintaining a privacy program.

While the state does not have a senior official responsible for maintaining a statewide privacy program to guide the development of a privacy incident response plan, state law tasks the State Chief Information Officer with developing information security policies and procedures, including developing and implementing policies for responding to events that threaten information systems or information stored on such systems.

We reviewed incident response policies and procedures that the state has in place to determine if they address the unique risks associated with incidents involving personal information.

We noted that there are processes in place to ensure agencies report a data breach once it has occurred — the statewide security incident response policy states that any incident relevant to the Oregon Consumer Information Protection Act should be reported to the incident response team at EIS. The Act defines what constitutes a breach of personal information and what needs to be reported to consumers and the state Attorney General if a breach of personal information occurs. EIS has also worked with other stakeholders to develop guidance on steps agencies should take to report an actual or potential data breach. However, statewide guidance does not address whether adjustments to incident handling processes should be considered when an incident involves PII to ensure a quick and effective response.

EIS has not developed a statewide training program for incident response

Once policies and procedures for responding to incidents involving PII are developed, they should be communicated to information system users based on their roles and responsibilities. Training may include incident simulations to test whether staff understand how to perform their roles effectively.

In Oregon, the State Chief Information Officer is responsible for developing and promoting information security training programs, but has not developed a training program to ensure agencies understand how to respond to security incidents involving PII. While this is in part due to a lack of statewide policies and procedures on which to base such training, management also indicated that they have not developed an incident response training program for agency staff because of ongoing changes in statewide security roles. For example, Senate Bill 90 in June 2017 restructured the state's information security function and moved information security personnel from state agencies to EIS.[8]

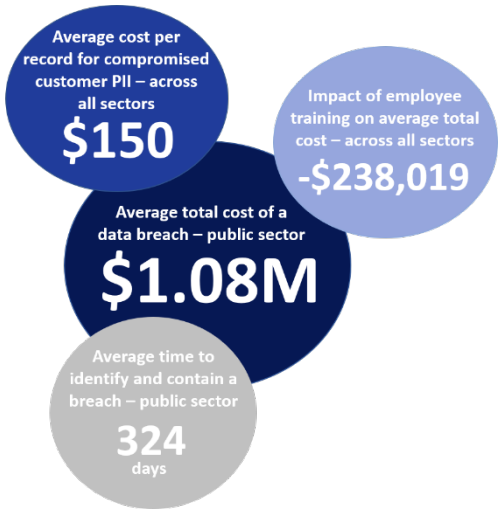
Currently, there are some inconsistencies in the roles and responsibilities outlined in statewide incident response plans, policies, and procedures. EIS is working with a consultant to help clarify and define roles and responsibilities across state entities, including those of agencies and the various divisions within EIS. In conjunction with this work, EIS is also in the process of revising statewide incident response policies and procedures to more accurately reflect current roles and processes.

Although EIS has not developed formal training on incidents involving PII, it has developed and implemented an annual statewide security training which agencies are required to take through the state's online training platform. The training provides some examples of reportable incidents and links to supporting guidance on how to report a security incident. However, it does not provide details on what steps an agency should take to analyze and contain an incident involving PII. EIS management stated that they also provide some ad hoc incident response training in response to security assessments or agency requests. Additionally, some agency leaders indicated that they provide training for their employees on disclosure and proper handling of sensitive information, such as federal tax information or health information.

[8] Senate Bill 90 "Transfers information technology security functions of certain state agencies in executive branch to State Chief Information Officer."

Without statewide policies, procedures, and training on how to respond to incidents involving PII, incident response personnel may not effectively, efficiently, and consistently respond to security incidents involving PII. For example, personnel responding to a security incident may inappropriately shut down a system, resulting in the loss of forensic data needed to resolve the incident. Additionally, incidents may continue to occur for longer periods of time before they are detected and contained. A 2020 study sponsored by IBM Security found that the average time for companies to detect and contain a breach was 280 days. The study found that, across 17 industry sectors, the public sector had the second highest amount of time to detect and contain a data breach, with an average of 324 days.[9] This can result in increased breach response costs and increased exposure of sensitive data.

Figure 6: The cost of a breach is quantifiable in time and dollars



Source: Ponemon Institute's 2020 Cost of a Data Breach Report (research sponsored by IBM Security).

The state's Chief Data Officer is making progress implementing enterprise data governance

Foundational data governance policy and strategy documents are in development

House Bill 3361 was enacted in August 2017 with an effective date of January 1, 2018. The bill charged the State Chief Information Officer with appointing a CDO to oversee enterprise open data standards set forth in the bill. Deadlines were established for some requirements, including:

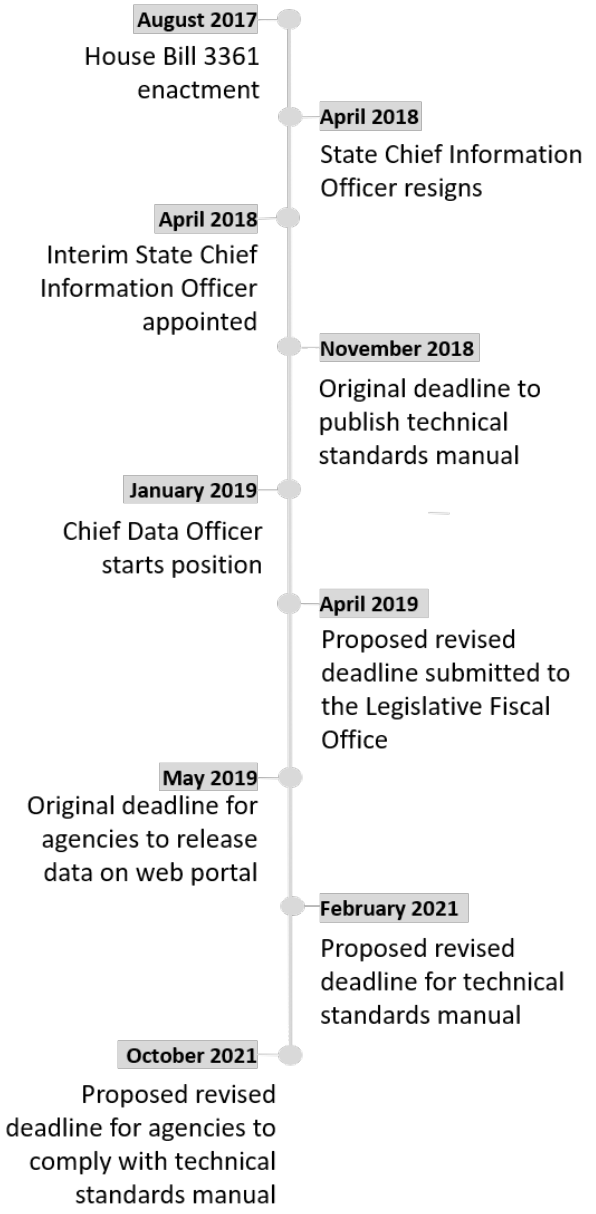
- November 5, 2018: The CDO shall first publish the technical standards manual for publishing data through the web portal maintained by the CDO; and
- May 1, 2019: Sections of the bill requiring release of publishable data and information management by state agencies become operative.

However, six months after the bill became effective, the State Chief Information Officer resigned before appointing a CDO. The state's Deputy Chief Information Officer stepped in as interim before being permanently appointed to the position in December of 2018. During this transition, the interim State Chief Information Officer performed a nationwide search for the CDO who started on January 14, 2019 — over two months after the first deliverable was due. The CDO is now working toward new deadlines to publish the technical standards manual by February 2021 and for agencies to comply with the manual by October 2021.

[9] The health care sector took the most time to identify and contain a data breach, with an average of 329 days.

The CDO's responsibilities include creating an enterprise data inventory, which is a key element to the open data initiative. Agencies, in turn, are responsible for creating and maintaining an inventory of their information resources that will be included in the statewide inventory. The CDO has developed draft guidance to assist state agencies in designing a method to inventory their data as well as a template to provide agencies with a standard format and methodology to inventory their information assets. A group of pilot agencies have begun to submit draft inventories; however, final guidance on initiating agency data inventories has not yet been released.

Figure 7: The State CDO started after the first deadline had already passed



Developing an inventory of data elements is a critical first step to managing privacy risk. Organizations must know what data they possess before they can effectively protect that data. While the CDO has made progress in creating an enterprise data inventory, they emphasized that the enterprise inventory created to comply with House Bill 3361 is intended to support the open data initiative. While the inventory template provided for agencies includes a field to indicate whether a data set contains PII, the inventory is not intended to support privacy risk management by providing a robust inventory of PII collected and stored by state agencies.

The CDO has also worked with an advisory group to develop a draft state data strategy. The first draft strategy was posted online for public comment from July 6 to August 24, 2020; a second draft was posted October 26 and is open for public comment through December 15, 2020. The state strategy emulates the 2020 federal data strategy in that it establishes principles, practices, and action items to better utilize data held by government agencies.

Oregon's draft strategy lays out 10 data principles and 36 data practices to create consistent and efficient data management across state agencies. The draft strategy includes practices to "preserve the privacy, quality, and integrity of data" by establishing "centralized privacy guidelines," and an action plan to outline how this will be achieved.

The CDO was also charged with providing information protection and privacy guidance for agencies; however, work has just begun on this requirement, as the CDO has prioritized development of the statewide data strategy and open data initiative in the office's first two years. See Figure 8 for the status on other tasks assigned to the CDO.

The CDO lacks resources to support agencies in fulfilling open data requirements effectively and efficiently

Figure 8: The CDO has made progress on privacy and data governance requirements

House Bill 3361 requirements	Status
§2 ¶2(d) Enterprise data inventory (publishable)	●
§2 ¶2(e) Data protection and privacy guidance	●
§2 ¶2(f) Enterprise data strategy	●
§2 ¶2(h) Strategies to combine internal/external data	✕
§2 ¶2(i) Statewide data governance and guidance	●
§2 ¶2(j) Education and standards for agencies	●
§2 ¶2(k) CDO advisory group and data sharing MOU	●

Legend: ● In-progress ✕ Not started

*Requirements summarized.

The first responsibility assigned to the CDO in House Bill 3361 is to maintain a central web portal on which agencies will release publishable data. However, the CDO may not have the human resources necessary to fully support agencies in their implementation of these requirements. Currently, the CDO is the only person in EIS working on the open data initiative. While EIS management expressed confidence in their ability to meet the CDO's deadlines, they also expressed concern that the office will not have the staff necessary to support agencies in publishing data on the open data portal.

In addition to establishing requirements for the CDO to publish the technical standards manual and maintain the open data portal, House Bill 3361 requires agencies to release publishable data on the web portal in accordance with the technical standards manual. According to EIS, agencies must comply with the open data standard and technical standards manual by October 2021. While the final standard is not expected to be published until February 2021; a draft version of the open data standard indicates that agencies must begin publishing data by June 2022.

However, EIS has identified a risk that the open data initiative may not be effectively and efficiently implemented without additional centralized support for agencies. Management believes there is an opportunity to support a more effective and efficient implementation of data publication by developing centralized resources to provide guidance, support, and where possible, process automation to agencies as they endeavor to publish their data sets.

When the open data initiative was first introduced to the Legislature in 2017, the request included only one position — the CDO. The initial request did not include funding for the personnel necessary to sustain the work. The Legislature voiced concern as to the sufficiency of the original funding request to support the open data initiative during a public hearing in 2017. EIS leadership at the time responded that the modest request was intended as a starting point. Current leadership is now developing a policy option package for the 2021 legislative session to request additional positions and technical resources.

While additional resources may help address the risk that agencies will not be able to effectively and efficiently publish data as required by House Bill 3361, the current budget environment is grim due to reduced state revenues as a result of COVID-19. Accordingly, additional funding in the 2021 legislative session may not be forthcoming. Because leading practices suggest that organizations should consider alternative responses to address an identified risk, it may benefit EIS to identify alternative strategies to support agencies in their efforts to comply with open data requirements set forth by the Legislature with current resources.

Recommendations

In order to develop an effective structure to manage enterprise privacy risk and ensure all agency personnel throughout the enterprise understand their role in responding to an incident involving PII, we recommend that EIS:

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.

Objective, Scope, and Methodology

Objective

The objectives for this audit were to:

1. Determine whether EIS has developed and implemented a governance structure to manage enterprise data privacy risk.
2. Determine whether EIS has provided policies, guidance, and training to ensure agencies understand their roles and responsibilities when responding to a security incident resulting in the unauthorized use or disclosure of personally identifiable information.
3. Determine the status of EIS' implementation of enterprise data governance and privacy-related requirements assigned to the state's CDO by the Legislature in 2017.

Scope

This audit focused on the governance structures in place to manage statewide privacy and incident response related to PII. Auditors also assessed the status of the CDO's efforts to implement enterprise data governance and privacy-related requirements set forth by the Legislature in 2017 (i.e., requirements established in House Bill 3361 in the 2017 Regular Session); we did not evaluate the sufficiency of internal controls for our assessment of the status of House Bill 3361.

Although privacy and information security overlap, this audit focused on privacy controls; we did not assess the sufficiency of information security controls.

While performing our audit, we considered the effects that COVID-19 may have on the audit topic.

The following internal control principles were relevant to our audit objectives:

- Control Environment
    - We considered whether the oversight body oversees the internal control system relevant to data privacy.
    - We considered whether management has established an organizational structure, assigned responsibility, and delegated authority to achieve the entity's objectives relevant to privacy and incident response related to PII.
- Risk Assessment
    - We considered whether management has defined objectives clearly to enable the identification of risks and define risk tolerances relevant to data privacy.
- Control Activities
    - We considered whether management has designed the entity's information system and related control activities to achieve objectives and respond to risks relevant to incident response related to PII.
- Information and Communication
    - We considered whether management internally and externally communicated the necessary quality information to achieve the entity's objectives relevant to incident response related to PII.

Methodology

To identify resources, policies, and procedures relevant to our audit objectives, we interviewed the following personnel:

- EIS State Chief Information Officer;
- EIS Cybersecurity management;
- EIS CDO;
- DOJ Assistant Attorneys General;
- Legislative Policy and Research Office analyst; and
- Compliance, technology, and security personnel at select agencies.

We also sent a survey to 20 judgmentally selected agencies to gain an understanding of the people and processes in place to manage data privacy risks at the agency level.

We inspected the following documents:

- Oregon Revised Statutes and Administrative Rules relevant to data privacy, incident response, and personally identifiable information;
- House Bill 3361 as enrolled by the Oregon Legislature in the 2017 Regular Session;
- Policies, procedures, and other materials provided by a selection of Oregon state agencies that are relevant to data privacy; and
- Statewide information security policies, procedures, and training materials.

To identify leading practices related to our audit objectives, we inspected the following documents:

- Federal laws and regulations relevant to data privacy;
- Federal privacy and data governance program materials; and
- Policies and procedures and governance structures established in other states that are relevant to data privacy, incident response, and personally identifiable information.

To identify generally accepted control objectives and practices for information systems, we used the National Institute of Standards and Technology's (NIST) Security and Privacy Controls for Federal Information Systems and Organizations and their Privacy Framework, the ISACA publication COBIT 2019 Framework – Governance and Management Objectives, and the United States Government Accountability Office's publication "Federal Information System Controls Audit Manual" (FISCAM). For internal control standards, auditors relied on "Standards for Internal Control in the Federal Government" published by the U.S. Government Accountability Office.

The map graphic used in this report for Figure 4 is used with the permission of the IAPP.[10] Data displayed in Figure 6 is used with the permission of Ponemon Institute; the research conducted by Ponemon Institute was sponsored by IBM Security.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We sincerely appreciate the courtesies and cooperation extended by officials and employees of DAS, EIS, and other agencies during the course of this audit.

[10] The source article and image can be found on IAPP's website at https://iapp.org/resources/article/state-comparison-table/.

Appendix A: Definitions

Data Breach – Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, protected data transmitted, stored or otherwise processed.

Data Lifecycle – The stages through which data passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion.

Data Privacy – There are many definitions of privacy, including "The right of a party to maintain control over and confidentiality of information about itself."

Information Security – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Event (as defined by EIS statewide policy) – An observable, measurable occurrence in respect to an information asset that is a deviation from normal operations.

Information Security Incident (as defined by EIS statewide policy) – A single or a series of unwanted or unexpected information security events that result in harm, or pose a significant threat of harm to information assets and require non-routine or preventative or corrective action.

Incident Response – The mitigation of violations of security policies and recommended practices.

Personally Identifiable Information (PII) – Any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person. A natural person being the person to whom the PII relates.

Personal Information (as defined in ORS 646A.602)

(12)(a) "Personal information" means:

(A) A consumer's first name or first initial and last name in combination with any one or more of the following data elements, if encryption, redaction or other methods have not rendered the data elements unusable or if the data elements are encrypted and the encryption key has been acquired:

(i) A consumer's Social Security number;

(ii) A consumer's driver license number or state identification card number issued by the Department of Transportation;

(iii) A consumer's passport number or other identification number issued by the United States;

(iv) A consumer's financial account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account, or any other information or combination of information that a person reasonably knows or should know would permit access to the consumer's financial account;

(v) Data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction;

(vi) A consumer's health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; or

(vii) Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer.

(B) A username or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the username or means of identification.

(C) Any of the data elements or any combination of the data elements described in subparagraph (A) or (B) of this paragraph without the consumer's username, or the consumer's first name or first initial and last name, if:

(i) Encryption, redaction or other methods have not rendered the data element or combination of data elements unusable; and

(ii) The data element or combination of data elements would enable a person to commit identity theft against a consumer.

(b) "Personal information" does not include information in a federal, state or local government record, other than a Social Security number, that is lawfully made available to the public.

Oregon
Kate Brown, Governor

Department of Administrative Services
Office of the Chief Operating Officer
155 Cottage Street NE
Salem, OR 97301
PHONE: 503-378-3104
FAX: 503-373-7643

November 12, 2020

Kip Memmott, Director
Secretary of State, Audits Division
255 Capitol St. NE, Suite 500
Salem, OR 97310

Dear Mr. Memmott,

This letter provides a written response to the Audits Division's final draft audit report titled: The State Does Not Have a Privacy Program to Manage Enterprise Data Privacy Risk.

Thank you for providing Enterprise Information Services (EIS) the audit report. We appreciate the work and collaborative approach of the Audits Division staff. We look forward to working on our response to the recommendation to enhance our commitment to improvement.

The State of Oregon information technology teams are decentralized. The systems are complex and retain information that require each agency to safeguard in accordance with many different entities. EIS submitted a Legislative Concept (LC) to establish a Chief Privacy Officer and staff. Should the LC continue to move forward and ultimately funded, EIS would begin to build an appropriate program in support of privacy overall. This concept is still in the approval process.

Below is our detailed response to each recommendation in the audit.

RECOMMENDATION 1

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.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**
Agree	2023	Terrence Woods 971-707-0233

Narrative for Recommendation 1
EIS agrees with the recommendation and is prepared to move forward if the Legislative Concept is eventually approved and funded. The target date will need to adjust depending on approval and availability of funds.

Please contact Lisa Upshaw, DAS Chief Audit Executive at 971-719-3114 with any questions.

Sincerely,

Terrence Woods
State Chief Information Officer

cc: Lisa Upshaw
Kathryn Helms
Jennifer Bjerke
Gary Johnson

Audit Team

Teresa Furnish, CISA, Audit Manager

Ian Green, M. Econ, CGAP, CFE, CISA, Audit Manager

Jessica Ritter, CPA, CISA, Senior Auditor

Sheila Faulkner, Staff Auditor

About the Secretary of State Audits Division

The Oregon Constitution provides that the Secretary of State shall be, by virtue of the office, Auditor of Public Accounts. The Audits Division performs this duty. The division reports to the elected Secretary of State and is independent of other agencies within the Executive, Legislative, and Judicial branches of Oregon government. The division has constitutional authority to audit all state officers, agencies, boards and commissions as well as administer municipal audit law.

This report is intended to promote the best possible management of public resources.
Copies may be obtained from:

Oregon Audits Division
255 Capitol St NE, Suite 500 | Salem | OR | 97310

(503) 986-2255
sos.oregon.gov/audits