SECRETARY OF STATE

AUDIT OVERVIEW

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

#2020-37

Presenter: Teresa Furnish, IT Audit Manager | Jessica Ritter, Senior IT Auditor

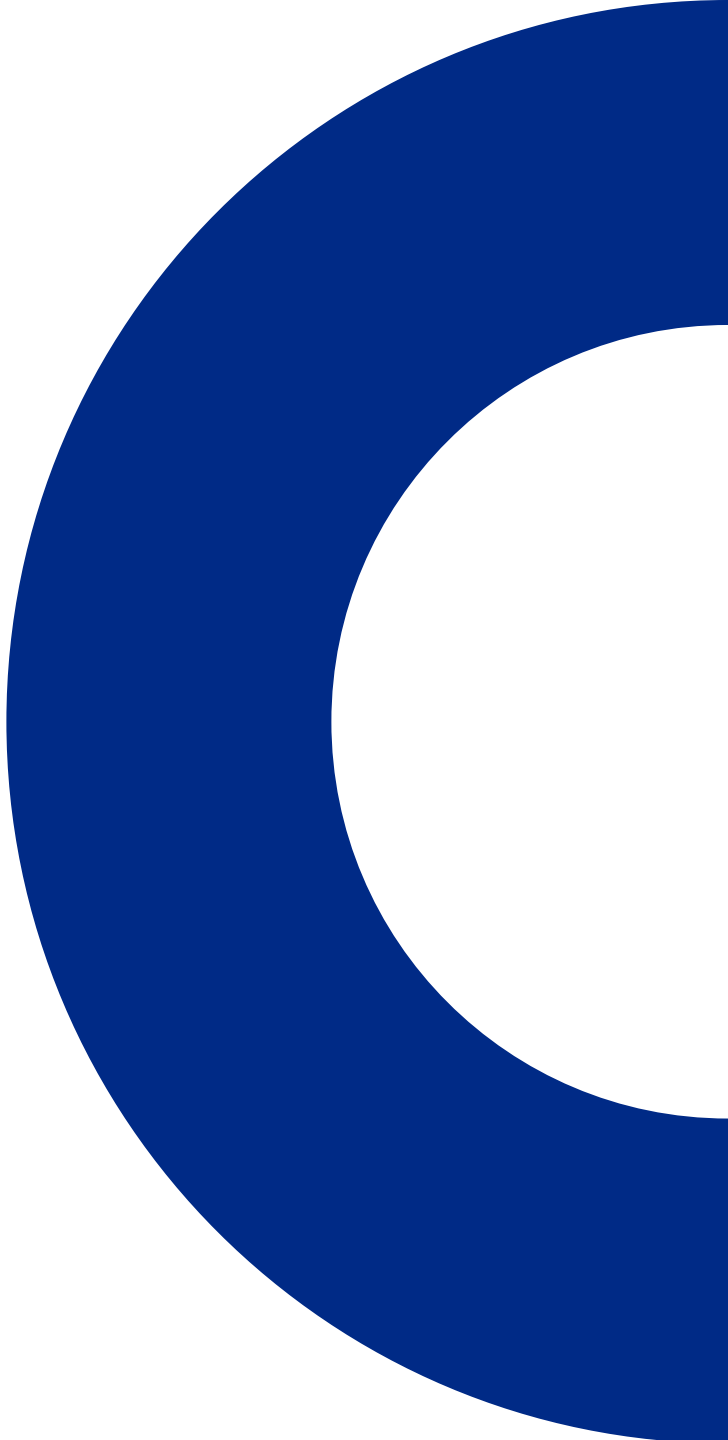
INTRODUCTION

- We performed this audit because:
  - Privacy and security concerns
  - Incohesive laws
  - Oregon House Bill 3361

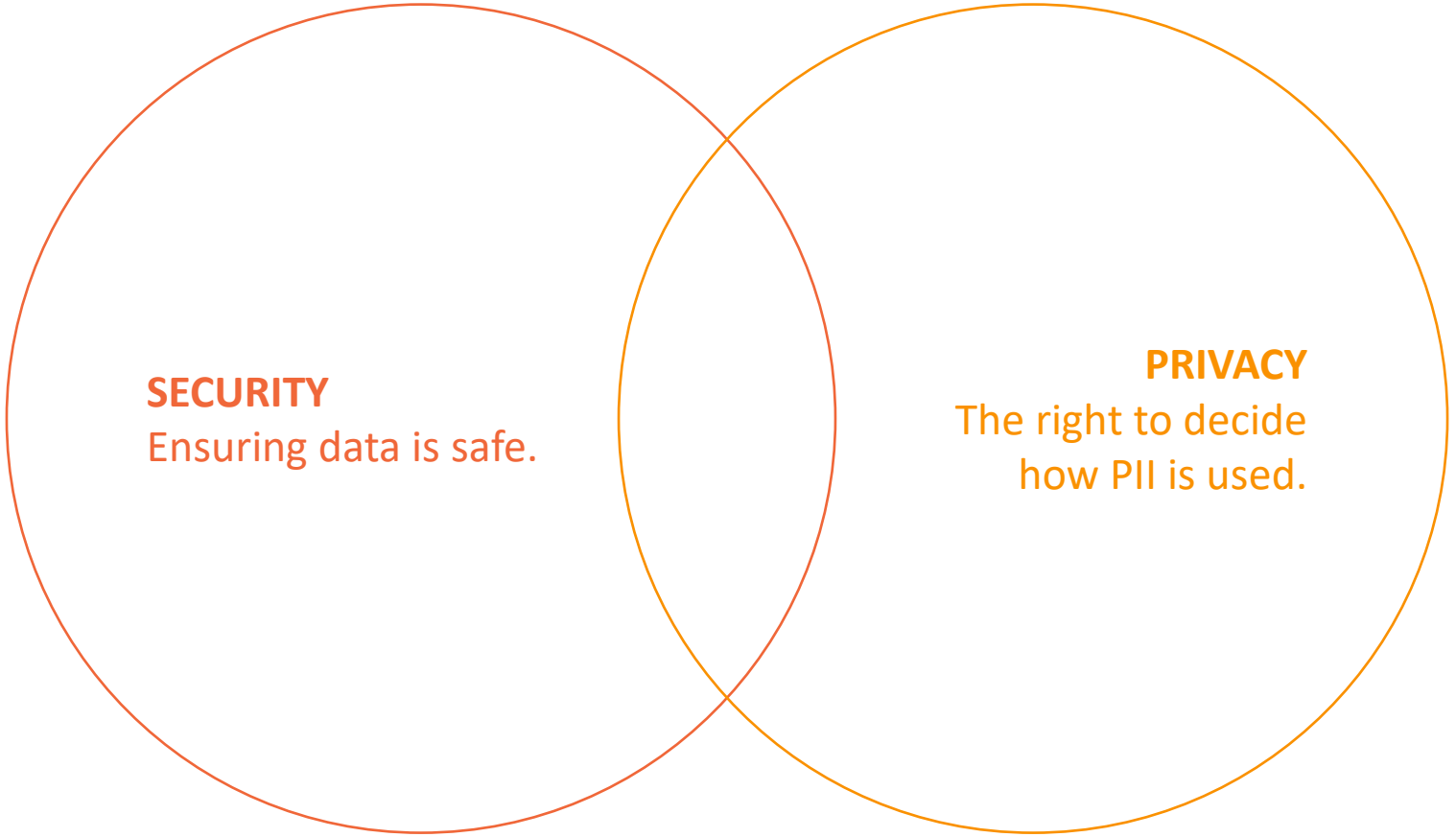
- Personally Identifiable Information (PII)

INTRODUCTION

- PII definition for this audit
- Not all PII is created equal
- PII collection



PRIVACY AND SECURITY



EVOLVING LAWS AND REGULATIONS

U.S. Privacy Act

The U.S. Privacy Act of 1974 includes restrictions on personal data held by federal agencies.

Social Security Act Amendments

Amendments set forth in 1990 bar disclosure of social security numbers collected on or after October 1, 1990

HIPAA

Health Insurance Portability and Accountability Act (HIPAA) includes protections for health information.

Universal Declaration of Human Rights

Includes Article 12: Right to Privacy.

FERPA

The Family Educational Rights and Privacy Act (FERPA) has protections for the confidentiality of student records.

DPPA

The Drivers Privacy Protection Act (DPPA) sets restrictions on disclosing personal information from a motor vehicle record.

All U.S. Citizens U.S. Industry Specific Geographically Specific

EVOLVING LAWS AND REGULATIONS CONT.

GLBA

Gramm-Leach-Bliley Act (GLBA) includes protections for financial nonpublic personal information.

Oregon Consumer Identity Theft Protection Act

Now known as the Oregon Consumer Information Protection Act, this law requires security safeguards for personal information.

CCPA

California Consumer Protection Act (CCPA) grants California consumers privacy rights and control over personal information.

COPPA

Children's Online Privacy Protection Act (COPPA) sets protections for children's online data (under the age of 13).

E-Government Act

The E-Government Act requires federal agencies to conduct Privacy Impact Assessments to demonstrate privacy protections have been incorporated.

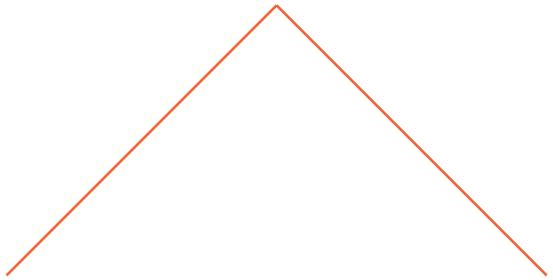
GDPR

General Data Protection Regulation (GDPR) sets protections and privacy principles in the European Union.

All U.S. Citizens U.S. Industry Specific Geographically Specific

ENTERPRISE INFORMATION SERVICES ROLE

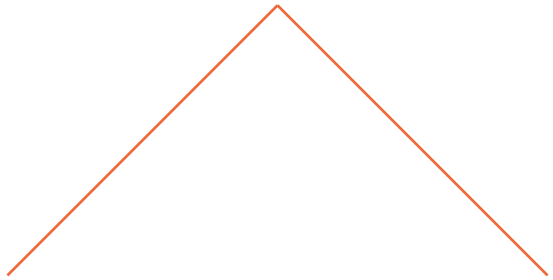
State Chief Information Officer



IT Governance

Security Across Executive Branch Agencies

Chief Data Officer



Data Governance Program

Transparency Program

OBJECTIVES

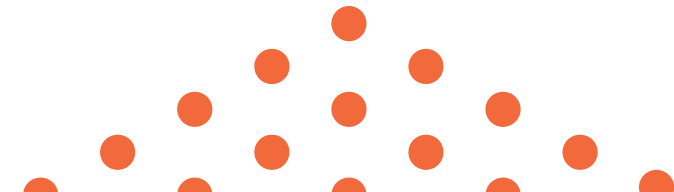
1. Determine whether EIS has developed and implemented a governance structure to manage enterprise data privacy risk.
2. Determine whether EIS has provided policies, guidance, and training to ensure agencies understand their roles and responsibilities when responding to a security incident resulting 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.

AUDIT RESULTS

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

AUDIT RESULTS

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

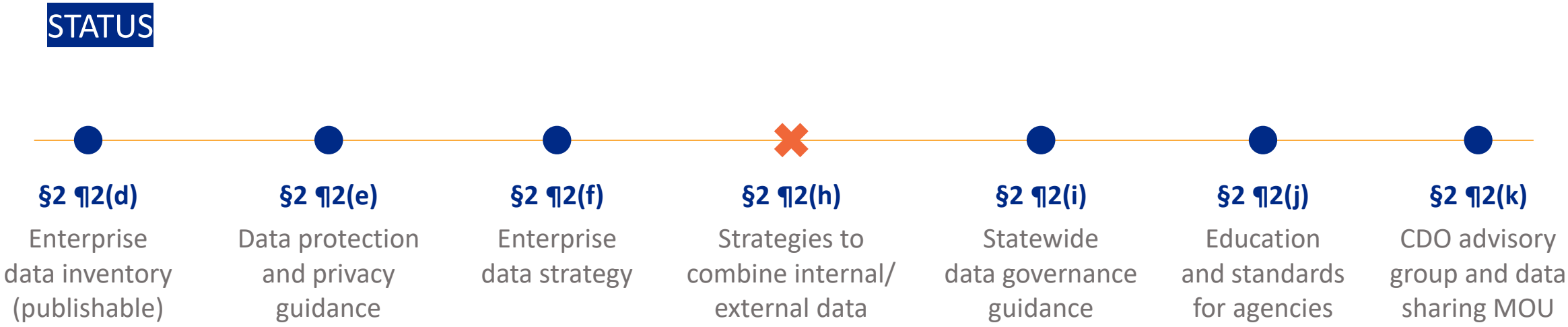


AUDIT RESULTS

The Chief Data Officer (CDO) is making progress implementing enterprise data governance

FIGURE 8: House Bill 3361 Requirements

The CDO has made progress on privacy and data governance requirements



RECOMMENDATIONS

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.

TERESA FURNISH, Audit Manager
Audits Division, Oregon Secretary of State
Teresa.L.Furnish@Oregon.gov

JESSICA RITTER, Senior IT Auditor
Audits Division, Oregon Secretary of State
Jessica.Ritter@Oregon.gov