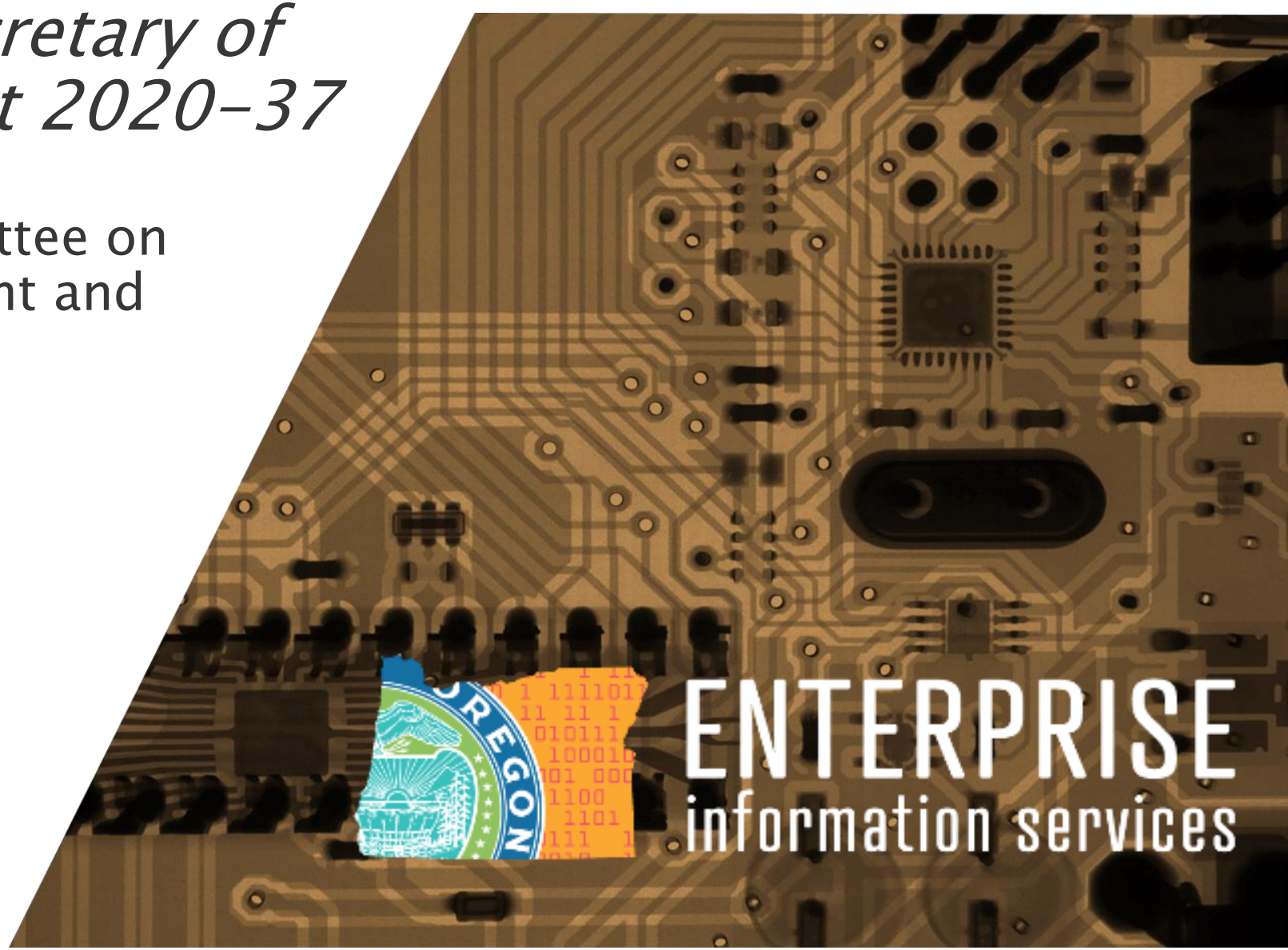
EIS Response. *Secretary of State Audit Report 2020-37*

Joint Legislative Committee on Information Management and Technology

Gary Johnson &
Kathryn Helms

3 March 2021



EIS Response. *Data Privacy*

GARY JOHNSON
Cyber Security Services

Chief Information Security Officer

KATHRYN HELMS
Data Governance and Transparency

Chief Data Officer

1. EIS Response to the audit recommendation
2. Evolving privacy landscape
3. Differentiating privacy—frameworks and key roles
4. Key capabilities and questions for a privacy program
5. Privacy and Open Data

Audit Recommendations. *EIS Response*

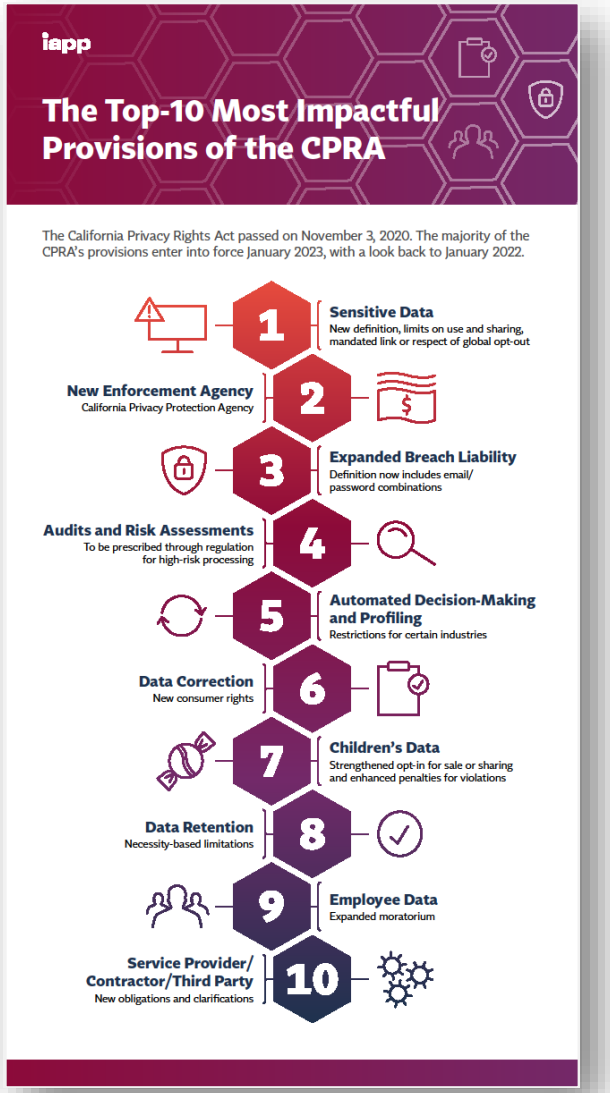
1. Request funding to establish a statewide privacy office and appoint a Chief Privacy Officer, or similar role, whose position will have the authority, mission, accountability, and resources to coordinate and develop statewide privacy requirements. Charge the CPO with the following tasks:

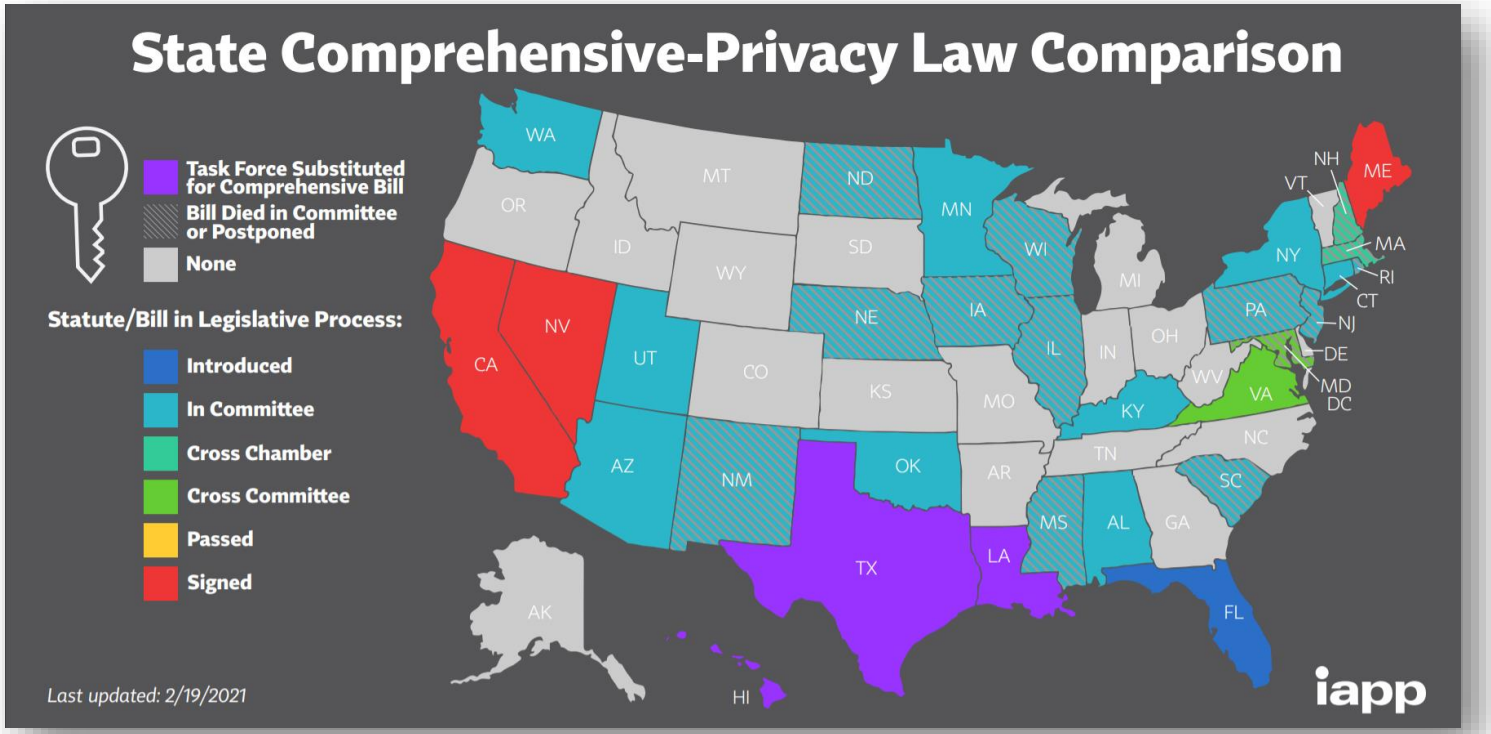
    a. Develop a strategic plan and timeline for coordinating an enterprise privacy risk assessment, developing statewide policies and procedures to manage and monitor privacy risk, and providing privacy training to agency personnel and third parties engaged in data processing;

    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.

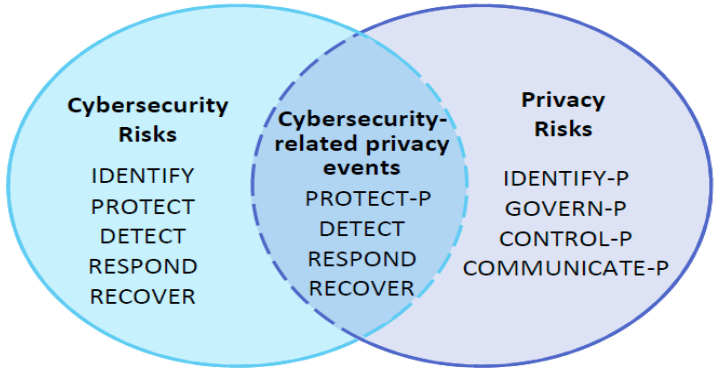
National Privacy Landscape. *Evolving Rapidly…*



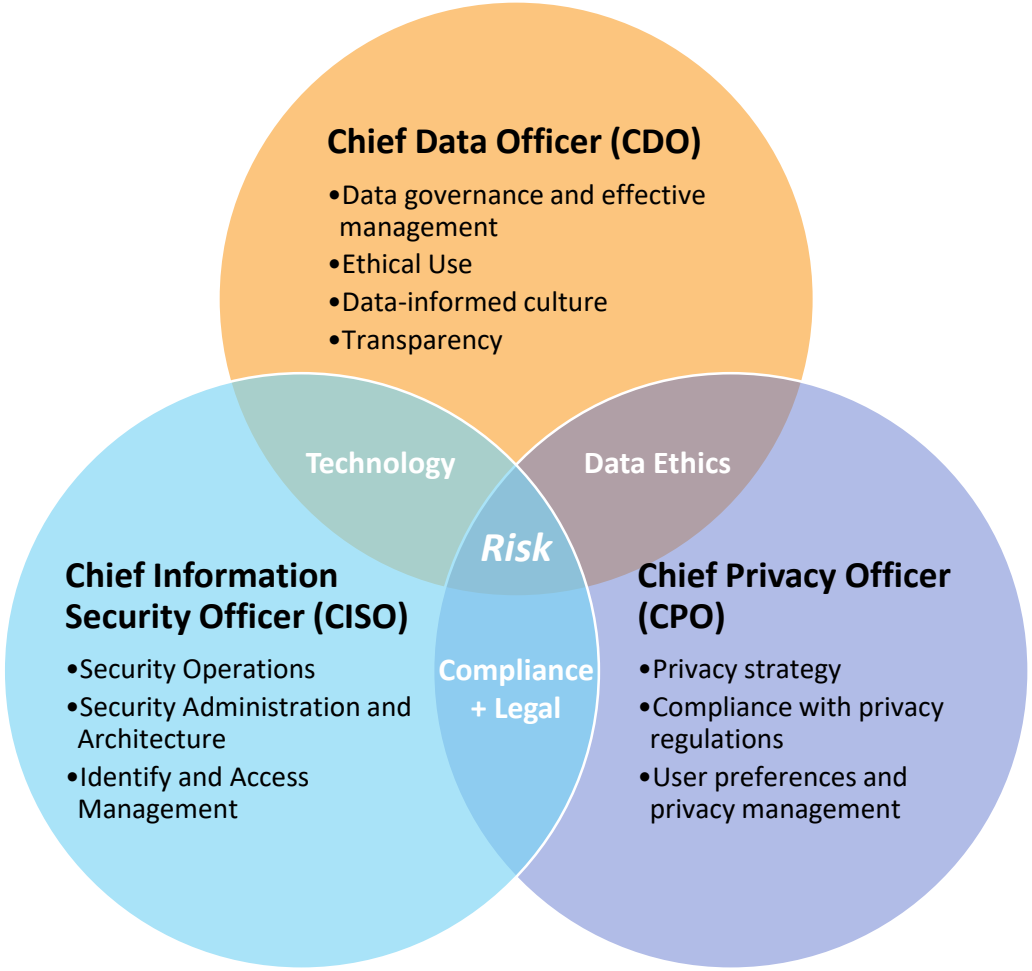


Differentiating Privacy. *Frameworks and Related Roles*

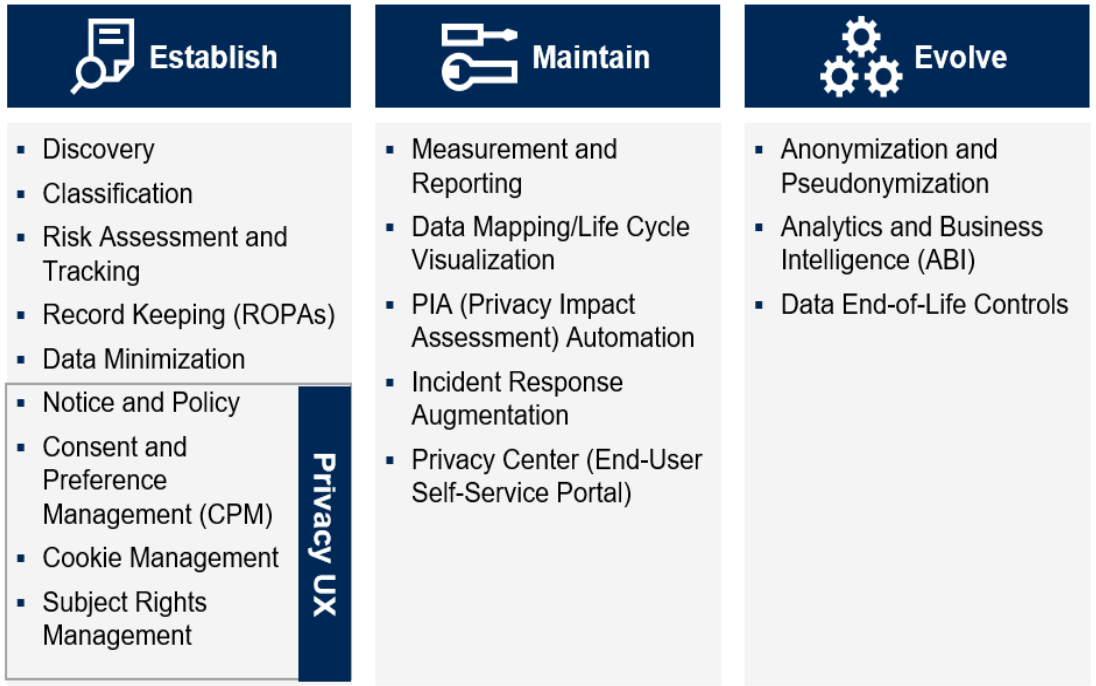
NIST Privacy Framework 1.0



- *"**Identify-P** – Develop the organizational understanding to manage privacy risk for individuals arising from data processing."*
- *"**Govern-P** – Develop and implement the organizational structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk."*
- *"**Control-P** – Develop and implement appropriate activities to enable an organization or individuals to manage data with sufficient granularity to manage privacy risks."*
- *"**Communicate-P** – Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how data are processed and associated privacy risks."*
- *"**Protect-P** – Develop and implement appropriate data processing safeguards."*



Privacy Program. *Key Capabilities and Questions*



Source: Gartner
ID: 376084

Source: Gartner (September 2019)
ID: 432939

Open Data Guidance. *Privacy for Open Data*

STEP 01

Identify sensitive or protected data elements

Note current privacy approach (if applicable)

STEP 02

STEP 03

Conduct benefit assessment (*benefit = potential benefit x likelihood*)

Identify the impact and risk of re-identification, and conduct a risk benefit analysis

STEP 04

STEP 05

Determine privacy approach; e.g., granularity, de-identification, and geo-masking

Conduct final open dataset risk assessment and publish (if applicable)

STEP 06

STEP 07

Planning and periodic reevaluation of datasets

Thank you.