AI in the Oregon Executive Branch

Nik Blosser
Chief Privacy Officer and
AI Strategist

Joint Committee on
Information Management
and Technology

November 18, 2025

Agenda

▶ Background: Privacy Report and AI Advisory Council

▶ AI and Privacy: Current State

▶ Opportunities

▶ AI Risk

▶ Implementation Status

"AI is not about replacing people, it's about augmenting human potential."
-- Fei-Fei Li, Stanford AI Lab

Background: Privacy Report (SB293 – 2021) and State Government AI Advisory Council

Privacy Report: SB293 (2021)

Senate Bill 293 (2021) directed EIS to evaluate and make recommendations regarding strengthening privacy and confidentiality. A report was delivered to the Legislature with the following five recommendations:

1. Establish the Chief Privacy Officer role.

2. Require the Chief Privacy Officer to develop and implement an Enterprise Privacy Program for the state of Oregon.

3. Create statutory authorization and budgetary authority for the Chief Privacy Officer.

4. Establish Privacy Program deliverables, including a privacy risk assessment tool for agencies.

5. Develop privacy outreach, education, and engagement strategies for the public.

These recommendations are still relevant, especially given the significant emerging interest in AI. To begin to address these recommendations as well as the AI Recommended Action Plan, the State CIO created a Chief Privacy Officer and AI Strategist role that began in September 2025.

AI Advisory Council Activities

▶ Executive Order No. 23-26 signed November 28, 2023

▶ Council convened and charter confirmed

▶ State benchmarking methodology overview

▶ National Institute of Standards and Technology definitions

▶ Draft Framework

▶ Public comment

▶ Subcommittees

    o Ethics

    o Equity

    o Security

▶ Final Recommended Action Plan delivered February 2025

AI Advisory Council Membership

- Terrence Woods, State Chief Information Officer, Council Chair

- Kathryn Darnall Helms, State Chief Data Officer

- Melinda Gross, Department of Administrative Services Cultural Change Officer

- Daniel Bonham, State Senator

- Daniel Nguyen, State Representative

- Jesse Hyatt, Executive Branch agency representative

Eight additional members, at the discretion of the Governor, may include community organizations with demonstrated expertise in data justice; artificial intelligence experts from Oregon universities; and representatives from local governments.

- Dr. Andres Lopez

- Catie Theisen

- Hector Dominguez Aguirre

- Janice Lee

- Justus Eaglesmith

- Ellen Flint

- K S Venkatraman

- Saby Waraich

AI Advisory Council Framework Guiding Principles

1. Accountability
2. Equity and Representation
3. Explainability and Trust
4. Governance
5. Human Oversight in AI Governance
6. Privacy and Confidentiality
7. Risk and Risk Management
8. Safety and Impact
9. Security and Securing
10. Stakeholder Experience and Equity
11. Transparency and Trustworthiness
12. Workforce Preparedness and Understanding

Final Recommended Action Plan: Five Executive Actions

1. Establish cross-functional AI governance framework

2. Acknowledge and address privacy concerns

3. Enhance security framework

4. Develop reference architecture

5. Address workforce needs

Recommended Action Plan High Level Roadmap

Initial activities ⟶ **Follow on activities**

Establish cross-functional AI governance framework	Execute updated Executive Order	Charter and appoint AI governance body	Develop core AI governance framework policies	Build partnerships
	Appoint AI leadership role	Establish decision making and roles	Establish feedback loops	Develop metrics and reporting
Acknowledge and address privacy concerns	Appoint privacy leadership role	Develop core AI privacy policies	Identify AI privacy impact assessment standards	Integrate data documentation requirements
	Develop templates for public disclosures	Identify AI documentation standards	Update agency data officer roles	Determine additional needs for continuing privacy efforts
Enhance security framework	Establish deactivation protocols	Scope and estimate data loss prevention capabilities	Implement NIST AI Risk Management Framework	Update agency incident response plans
	Review and update security policies	Update vendor requirements	Update statewide incident response plan	
Develop reference architecture	Publish AI use case inventory	Pilot AI risk management framework	Recommend AI testing framework	Develop power management policies
	Define initial AI reference architecture	Establish cross-agency advisory group	Establish minimum performance standards	
Address workforce needs	Evaluate workforce impacts	Research existing training	Develop state procurement training for AI contracts	Create shared resource webpage
	Engage Workforce and Talent Development Board	Deliver human in the loop training	Develop employee AI training	Partner with universities for innovation labs

ENTERPRISE
information services

"AI will change society more than electricity or the internet."
-- Geoffrey Hinton, computer scientist
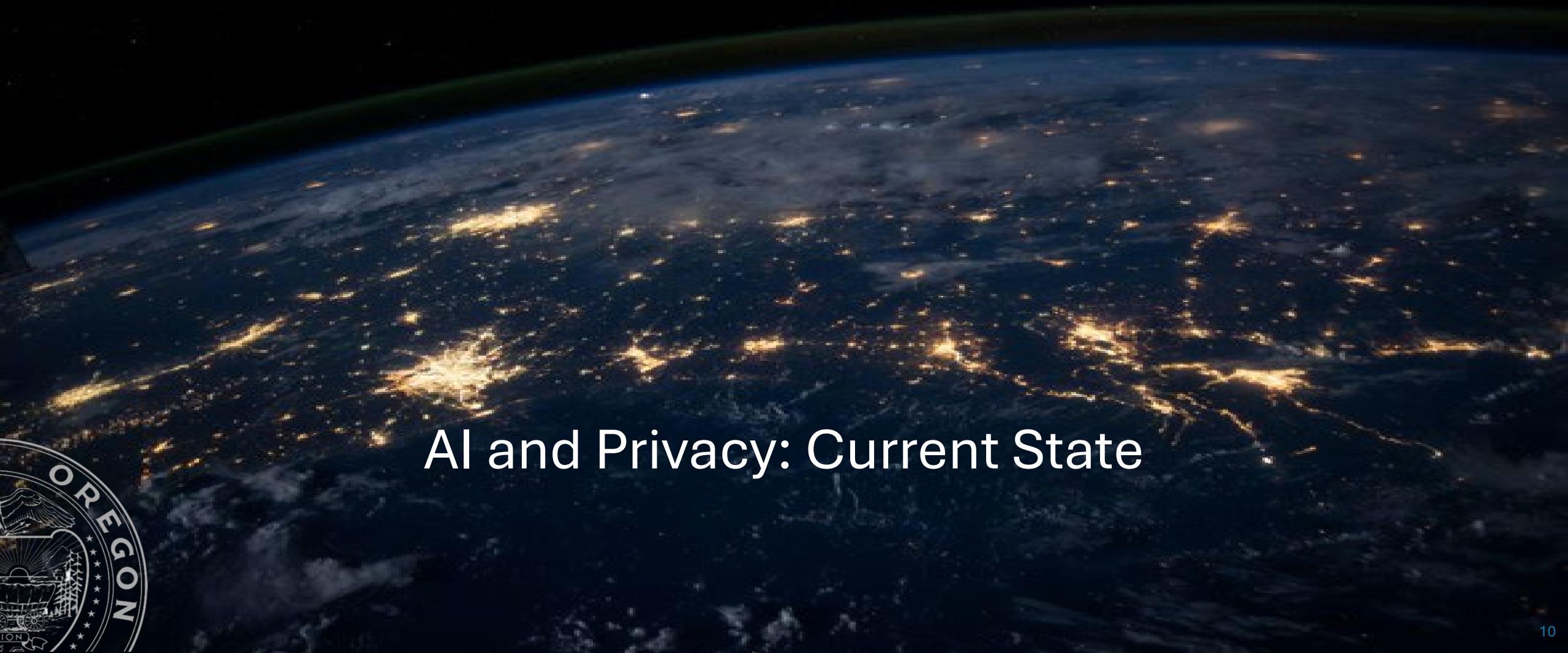
AI and Privacy: Current State

# A majority of Americans say they interact with AI at least several times a week

"% who say they interact with artificial intelligence (AI)..."

62%

	Almost constantly/ Several times a day	About once a day	Several times a week	Less often
U.S. adults	31	15	17	38
Men	33	16	17	33
Women	28	14	16	42
White	31	15	17	37
Black	27	18	13	41
Hispanic	29	13	16	42
Asian*	39	19	18	24

Ages 18-29	33	20	21	26
30-49	37	16	14	33
50-64	30	13	18	39
65+	19	11	16	54
Postgrad	46	16	17	21
College grad	39	17	19	25
Some college	30	15	17	37
HS or less	20	14	14	51
Rep/Lean Rep	28	15	18	40
Dem/Lean Dem	33	15	16	35

Report: How Americans View AI and Its Impact on People and Society
- Pew Research Center, June 2025

Americans express varying degrees of support for AI playing different roles in society

"% of U.S. adults who say AI should play __ in each of the following areas"

Report: How Americans View AI and Its Impact on People and Society
- Pew Research Center, June 2025

12
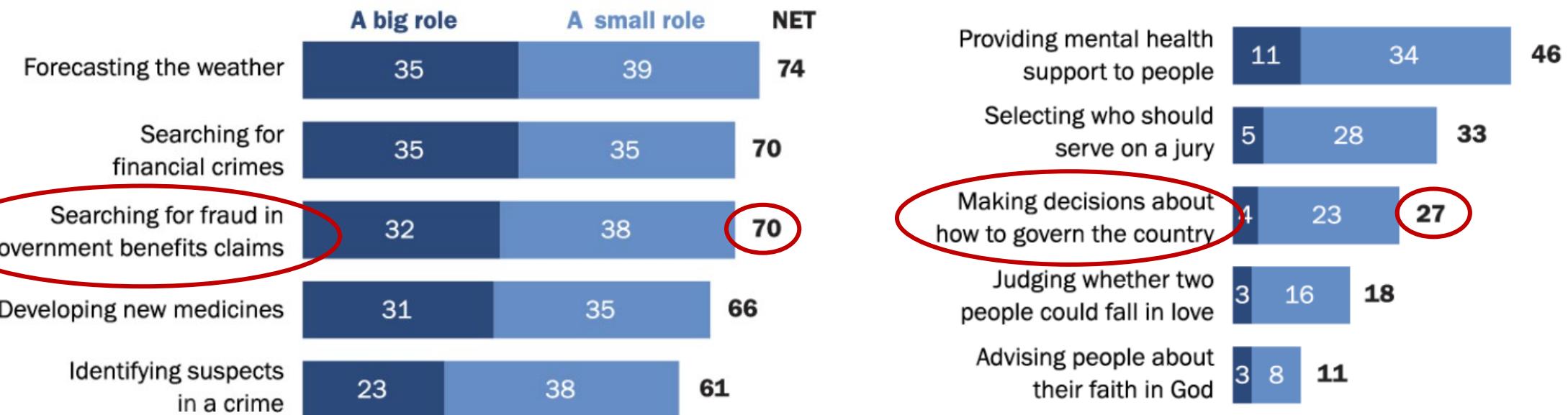
CURRENT STATE: How we're implementing AI at state agencies:

[Updated Interim Generative AI Access and Usage Guidance](#) (September 12, 2025)

Key directives:

➢ **Data classification and protection is critical:** both for enabling AI tools and for protecting restricted data; <u>only level 1 (Published) and level 2 (Limited) data currently allowed</u>

➢ **A human must be in the loop** – reviewing AI-generated content before use

➢ **User training** and **agency monitoring of compliance**

➢ **EIS is responsible for reviewing and approving all AI systems and use cases** by executive branch agencies

Current recommended uses from [Updated Interim Generative AI Access and Usage Guidance](#)

Recommended Use of Generative AI

✔ = recommended, **Supervisor**=With approval, X= not recommended

Breadth of Distribution	Proofreading, Grammar	Brainstorming/ First Draft <25% AI	Collaborative Writing About 50% AI	Human Edited >75% AI	Copy-paste generated Content
Press release, prepared remarks	✔	Supervisor	✗	✗	✗
Replies to public inquiry	✔	Supervisor	✗	✗	✗
Public facing web content	✔	Supervisor	Supervisor	✗	✗
Memos, broad internal comm	✔	Supervisor	Supervisor	✗	✗
Internal process docs	✔	✔	Supervisor	✗	✗
Source code	✔	✔	Supervisor	✗	✗
Emails	✔	✔	Supervisor	Supervisor	✗
Chat	✔	✔	Supervisor	Supervisor	✗

Opportunities

With the right training, oversight, data and usage, AI can be amazing at supporting employees:

Initial use cases – internal facing and no use of restricted/regulated data
Finding a "needle in a haystack" – natural language queries of large, organized knowledge bases, such as policies, rules, statutes (example: Eligibot from OHA/ODHS)
Analysis of large amounts of text or numbers – public comments, federal reports, managing records requests, document classification and routing
Writing (language) – brainstorming, collaborating, drafting, proofreading, editing - Everything from press releases and remarks, web content, letters - Template-based document generation: letters, notices, procurement, reports, etc.
Writing (computer code)
Transcription and summarization – meetings, voicemails

Approved AI Tools for state agencies (November 2025)

Approved tool	Used for	Available to	Approval process
Copilot Chat	Personal productivity	All state employees	Already approved
M365 Copilot	Enhanced personal productivity	Employees with additional license and training	Agency can approve
GitHub Copilot	Writing/editing computer code	Employees with license	EIS review
Copilot Studio	Building an agent without coding	Beginning training program in Dec 2025	EIS review
Azure Foundry AI	Building an agent – requires coding	IT shops at large agencies	EIS review
All other tools	Specific agency use cases	Varies	EIS review

Current state employee trainings in Workday and the M365 Hub

- o Title: **Responsible AI for Public Professionals**
- o Creator: **Innovate-US**
- o Facilitator: **Self-paced**
- o Duration: **~ 2 hours**
- o Topics include:
  - Practical use of GenAI in your day-to-day work
  - Ethical and responsible AI practices
  - Improving public service delivery with AI
- o Access this training in **Workday Learning** by searching for DAS – EIS – Responsible AI for Public Professionals

- o Title: **Copilot video trainings from Microsoft**
- o Facilitator: **Self-paced**
- o Duration: **~ 1 hour each**
- o Topics include:
  - Copilot Chat Training
  - M365 Copilot and Advanced Prompting
  - Copilot in Outlook and Teams
  - Copilot in Word and Excel
  - Copilot in PowerPoint and OneNote
- o State agencies access this training in **Microsoft M365 Hub** at the Video Training Library.

"It's sophisticated software mimicking human interaction patterns."
-- Dr. Matthew Nour, Oxford University

AI Risk

AI Risks... and some mitigations

Risk	Mitigation
Hallucinations in AI output (safety, accuracy)	Make sure a human reviews and verifies content; improved prompting to enforce accuracy
Data breaches of confidential data	Numerous, including data classification, data controls, use of data loss prevention (DLP)
Insufficient "human in the loop" (accountability, equity and representation)	Document processes where AI is involved and specify where and how human oversight occurs
Employee use of unauthorized, unapproved or dangerous AI tools	Block network access
Emerging cyber threats – "prompt injections"	Training
Lack of transparency and trust	Transparent governance; communication plans; attention to budget risks with any new technology
Lack of workforce preparedness and understanding	Training and investment in change management
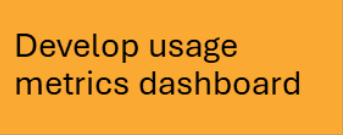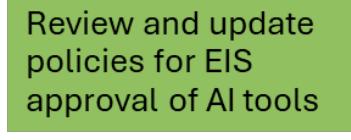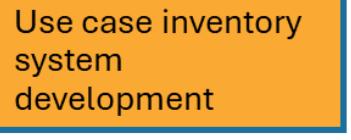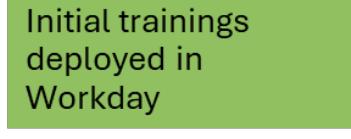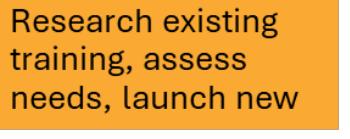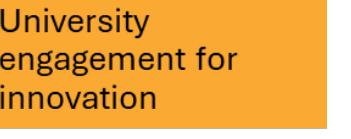
Plato was famously very skeptical of writing because it would harm your memory. And guess what – it did.
- Phaedrus
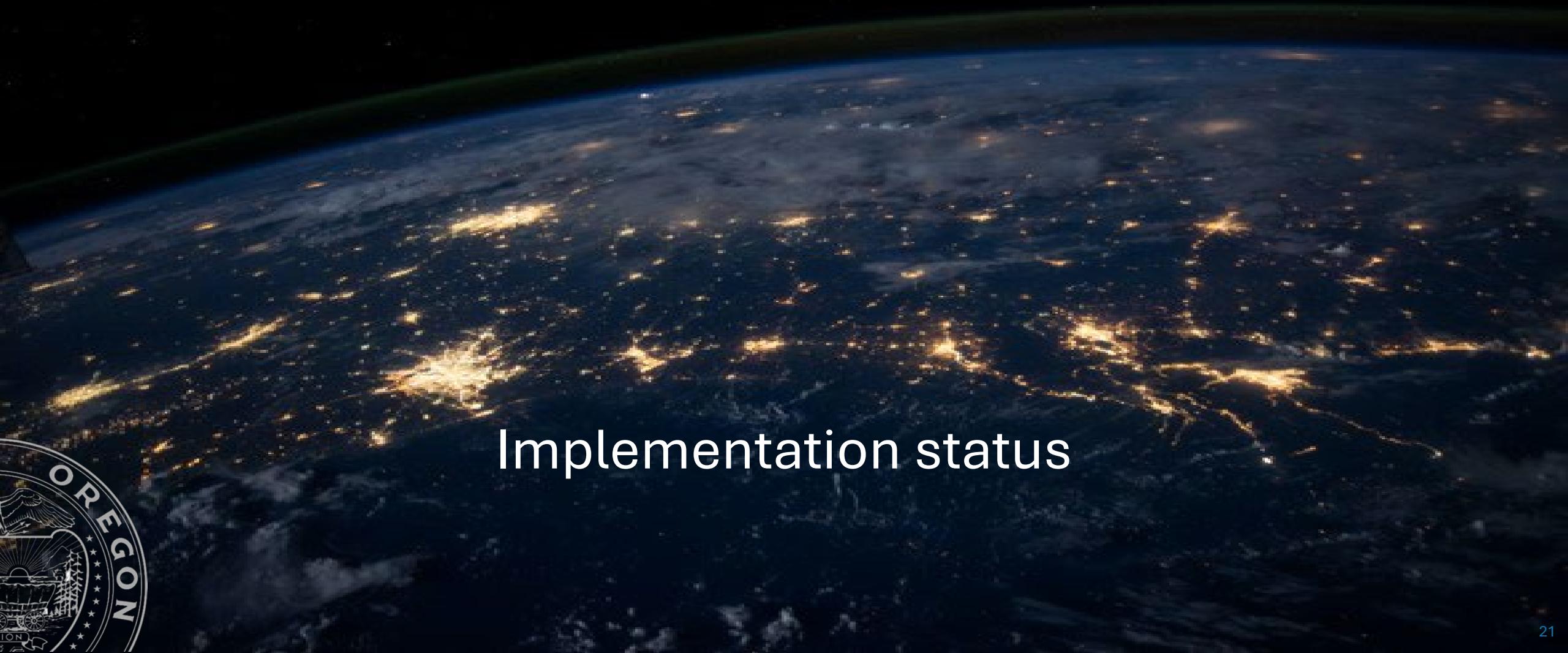
Implementation status

Roadmap implementation status

	Completed	In process		
Establish cross-functional AI governance framework	Appoint AI leadership role	Develop usage metrics dashboard		
Acknowledge and address privacy concerns	Appoint privacy leadership role	Privacy program development		
Enhance security framework	Review and update policies for EIS approval of AI tools	Data loss prevention implementation		
Develop reference architecture		Use case inventory system development	AI risk management framework development	
Address workforce needs	Initial trainings deployed in Workday	Agency leadership engagement	Research existing training, assess needs, launch new	University engagement for innovation
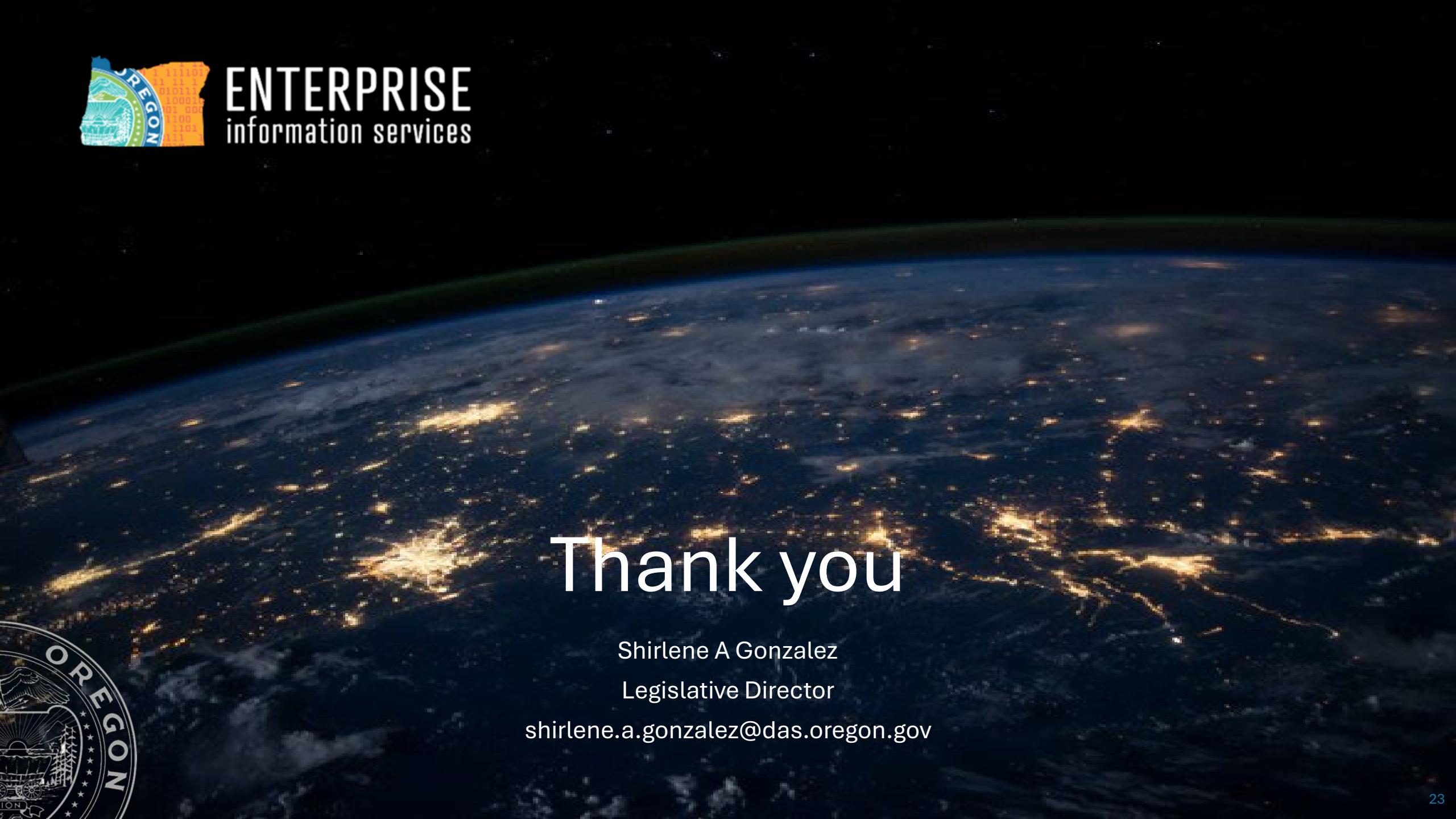
Thank you

Shirlene A Gonzalez

Legislative Director

shirlene.a.gonzalez@das.oregon.gov