State Government Artificial Intelligence Advisory Council Final Recommended Action Plan

FEBRUARY 4, 2025

Contents

Executive Summary

In response to the growing role of Artificial Intelligence (AI) within society, on November 28, 2023, Governor Tina Kotek established the Oregon State Government Artificial Intelligence Advisory Council (AI Council).[1] Tasked with guiding the responsible adoption of AI in state government, the AI Council's primary purpose was to develop a final recommended action plan to guide the awareness and thoughtful adoption of AI within Oregon state government. Through these efforts, the AI Council aims to foster a future where AI improves public services, increases trust, and supports economic and environmental sustainability.

The AI Council first convened on March 19, 2024, and met publicly to discuss and develop the AI framework. Beginning in June 2024, the AI Council created three subcommittees to address core principles related to AI: security, ethics, and equity, with each subcommittee drafting principles and recommendations. The AI Council released a recommended plan and framework on September 13, 2024, which included 12 guiding principles and 74 recommendations. The AI Council, with support from Enterprise Information Services staff, elaborated the framework into five key strategic recommendations with concrete executive actions, policies, and investments.

The AI Council Final Recommended Action Plan is organized to include:

- An initial vision for how Oregon state government wishes to use, adopt, and advance AI technologies in alignment with Oregon's values of diversity, equity, and inclusion.
- Guiding principles for how Oregon state government will use, adopt, and advance AI technologies. These guiding principles serve as commitments the AI Council considers foundational in developing a strong AI strategy for state government.
- The following five strategic recommended executive actions are presented with supporting high level tasks, each with a suggested accountable role and estimated timeframe to accomplish, and estimated needed resources and investments.
    1. Establish a cross-functional AI Governance framework that ensures human-in-the-loop oversight, prioritizes equity and ethics, and aligns with Oregon's values of diversity, equity, and inclusion.
    2. Acknowledge and address privacy concerns with leadership and resources to conduct comprehensive privacy impact assessments for AI systems.
    3. Enhance the security framework to include AI-specific incident response protocols and risk management strategies.
    4. Develop a reference architecture and policies for the acquisition, development, testing, and auditing of AI systems.
    5. Address workforce needs through training programs, partnerships with academic institutions, and clear guidelines for AI implementation.

This final recommended action plan represents eleven months of effort through AI Council meetings, subcommittee work, benchmarking research, and engagement with peer states and government AI communities of practice. Early in their work, the AI Council decided to utilize

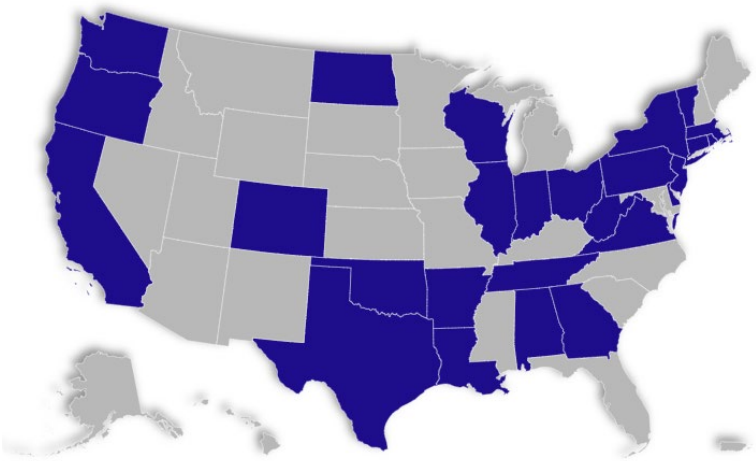
[1] https://www.oregon.gov/gov/eo/eo-23-26.pdf

National Institute of Standards and Technology definitions as their anchor for reference and consistency.[2] The framework focuses on safety and security, workforce education, transparency, privacy, equity, and ethics as critical to Oregon government's use of AI. Through these coordinated efforts, Oregon aims to position itself as a leader in responsible AI adoption while maintaining public trust and ensuring equitable outcomes for all Oregonians.

Background

In creating the State Government Artificial Intelligence Advisory Council (AI Council), Oregon joined many peer states in recognizing AI's capacity to shape society, economy, and culture in unintended and unanticipated ways if its adoption is not carefully stewarded. AI has the potential to improve efficiency, increase accessibility of information and services, enhance the constituent experience, and support improved decision-making. However, AI is only as intelligent as the data, developers and designers that create it, and AI technologies require consistent ingestion of high quality, timely data to maintain accuracy and usability. Absent careful adoption, monitoring, and oversight, AI systems can pose significant risks to individuals' civil and human rights, discriminate towards marginalized populations, produce misleading and harmful information, misguide users, result in harmful targeting and surveillance, and degrade trust in government institutions.

Figure 1: States who have created an AI Task Force or Council[3]



Development and maintenance of AI models and tools frequently have additional labor and climate impacts outside of deployment. AI requires immense computing and infrastructure resources, with the International Energy Agency estimating electricity consumption from data centers and the AI sector to double by 2026[4]. AI is dependent upon human labor to support data cleaning, coding, labeling, and classification. This commonly labeled "ghost work"[5], (human work that is often made invisible in the development of AI) presents a currently unregulated global marketplace where workers perform tasks such as flagging violent or explicit images, moderating social media content,

[2] https://airc.nist.gov/AI_RMF_Knowledge_Base/Glossary
[3] https://www.govtech.com/biz/data/is-your-government-ai-ready-an-interactive-tracker-of-ai-action
[4] https://www.iea.org/reports/electricity-2024/executive-summary
[5] https://www.noemamag.com/the-exploited-labor-behind-artificial-intelligence/

or reviewing training data, for wages as low as $1.46/hour. These societal impacts across labor, workforce, and environment further underline the need for Oregon to set forth a vision to incorporate ethics, equity, and impact into how it leverages AI to ensure Oregon maintains its values of environmental stewardship and economic sustainability. Fundamental to ethical adoption of AI is the preservation of Oregon's values of diversity, equity, and inclusion in Oregon's AI development lifecycle. The principles and recommendations within this action plan highlight the critical importance of including the lived experiences and voices of those most likely to be impacted by an AI solution, from recognizing the workforce impacts for state employees who may be using these technologies, to ensuring that community and public participation are incorporated into development of any future ethics or equity frameworks guiding AI development.

Oregon's Artificial Intelligence Vision and Principles

The vision statement and guiding principles within this action plan represent the strategic vision and goals of Oregon's approach to AI, as well as recommendations for how Oregon's policies, programs, and guidance will be developed and implemented. In creating AI principles, Oregon hopes to guide the effective design, use, and implementation of AI systems, similar to the White House's AI Bill of Rights, as released by the Office of Science and Technology Policy in October 2022. Oregon's principles are drawn from internal benchmark efforts[6] and analysis across multiple government and public interest organizations, such as the White House AI Bill of Rights, the Organization for Economic and Cooperative Development's AI Principles, and the European Union.

Vision Statement

Create an informed and empowered workforce where state employees are well-equipped and trained with the knowledge and understanding of AI to make informed decisions. We envision a future where AI is governed by transparent, well-defined policies that ensure its ethical use, promote diversity, equity, and inclusion, and safeguard personal and sensitive information. Oregon aims to foster a responsible AI ecosystem that enhances government efficiency, accountability, and public trust, while upholding the highest standards of privacy and ethical integrity.

Oregon's Artificial Intelligence Guiding Principles

1. **Accountability:** AI systems are subject to continuous audits measuring fairness, accuracy, safety, and efficiency, with clear reporting to Oregonians.
2. **Equity and Representation**: AI systems clearly explain decision-making processes to users and affected parties through accessible and transparent communication.
3. **Explainability and Trust**: AI systems deployed by the state should be developed and implemented with transparent methodologies, data sources, and design procedures. Those asked to engage with AI or have their data used by AI should do so with informed consent. AI decision-making processes must be clearly explained to both users and affected individuals.
4. **Governance**: Policies, processes, procedures, and practices across the Executive Branch related to the mapping, measuring, and managing of AI benefits and risks are in place,

[6] https://www.oregon.gov/eis/Documents/SG%20AI%20Advisory%20Council%20Meeting%20Materials%20240611.pdf

transparent, and implemented with accountability and full inspection; a culture of risk management is cultivated and present.

5. **Human Oversight in AI Governance**: Define clear structures and governance on how human oversight will be intentionally built into the adoption, review, and day-to-day implementation of AI. Clearly defined roles and responsibilities on this and the overall governance and decision-making of how, where, and when AI systems are adopted and utilized is critical.
6. **Privacy and Confidentiality:** Prioritize public privacy protections in AI systems and clarify oversight responsibilities, especially in smaller agencies; safety -related or emergency data use is subject to extra review.
7. **Risk and Risk Management:** Identify, assess, measure, and manage all AI risks, ensuring compliance with relevant regulations and assessing projected impacts.
8. **Safety and Impact:** AI design and use do not decrease overall safety. Specify impact and safety requirements with quantifiable terms and measurement methods.
9. **Security and Securing**: AI system's design, use, and lifecycle management protect it and its data from unauthorized access, alteration, or destruction.
10. **User Experience:** AI should be utilized as a tool to improve the efficiency of implementers and improve the constituent experience, not adopted as a default solution. Adoption and use of AI tools will be guided by critical consideration of the use case identified, constituent experience, and subject matter expertise within the organization.
11. **Transparency and Trustworthiness:** Ensure clarity, openness, comprehensibility of AI processes, outcomes, impact, and decision background. Document and share all lifecycle steps of AI system development with the public and impacted persons. AI design and use justify public trust through accountability and timely communication.
12. **Workforce Preparedness and Understanding**: Workers incorporating AI systems into their workflow should be a part of the adoption decision and review processes and be adequately informed and trained to appropriately utilize the system. In addition, it's critical that Oregon's next generation of workers have a baseline of education in AI – both in a broader framework of what is possible with AI, ethical considerations and implications, and direct and practical applications.

Final Recommended Action Plan

The following describes the recommended executive actions. For each of the recommended executive actions, an appendix further elaborates high level tasks with a recommended accountable role, proposed estimated timeframe, as well as resources and investments needed to initiate each recommendation. Identified positions are dependent on position authority and funding. Further elaboration and refinement are expected with the development of an implementation plan for each recommendation.

Key tasks include executing an updated Executive Order, appointing AI governance leadership, and establishing interim decision-making frameworks. Subsequent and parallel tasks include developing comprehensive policies, training programs, and oversight mechanisms. Future activities will likely include advanced governance tools and continuous improvement frameworks.

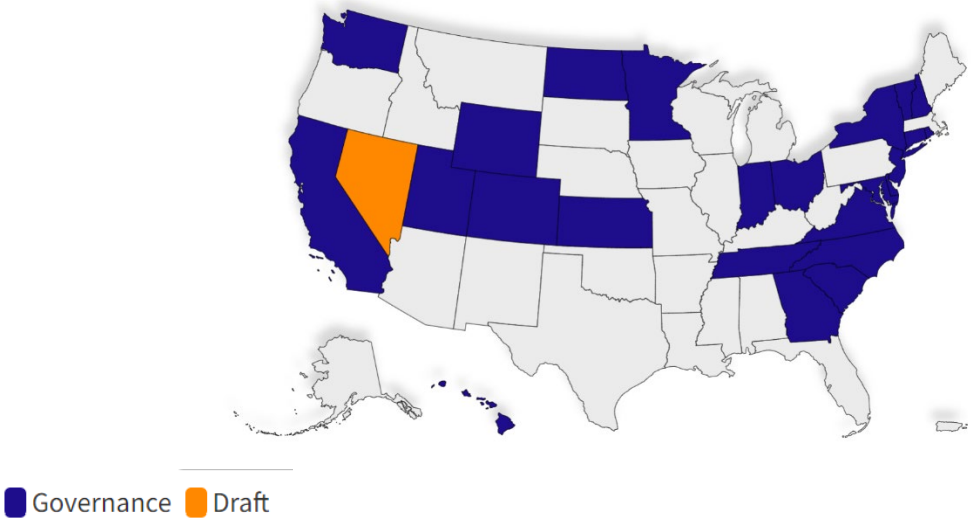
Establish cross-functional AI governance framework that requires human-in-the-loop oversight in the adoption and deployment of AI and decision-making systems, especially in areas impacting safety, equity, and ethics. (Addresses the following recommendations from the draft framework 1.2, 2.1, 2.4-2.13, 4.5-4.7, 5.1, 8.1, 8.2, 10.2, 11.2, 11.6, 12.3, 12.4, 12.6 referenced in Appendix G.)

The recommended AI governance framework responds to potential equity and ethical concerns by designating governance roles and decision-making structures, clarifying accountability, and integrating standardized policies for transparency. Key elements focus on addressing biases, fostering equitable data practices, sustaining open communication with community stakeholders, and specifying safety requirements. The AI governance framework also emphasizes collaboration with academic, industry, and nonprofit partners to share expertise, expand training opportunities, and pilot AI tools aligned with ethical standards. Over time, metrics and audits will help track progress, refine policies, and ensure the AI governance framework remains effective. Through this structured approach, state government aims to balance innovation with fairness, accountability, and stakeholder trust in its AI systems.

Effective AI governance combines ethics, responsible AI policies and AI technology to achieve responsible AI, trust and innovation. By establishing clear roles, consistent oversight, and processes that integrate worker and community perspectives, this framework provides a foundation for responsible AI use. As AI technology evolves, these guidelines are designed to adapt and safeguard equity, transparency, and accountability. Approaches to AI must also involve collaboration with, and understanding of, Oregon's sovereign tribal nations and recognition of indigenous data sovereignty, as well as community self-determination. Through ongoing collaboration, audits, and training, the state will maintain a governance model that balances innovation with the public interest.

High level tasks and resources needs are provided in Appendix B.

Figure 2: States with AI governance.[7]



Acknowledge and address privacy concerns with leadership and resources to conduct privacy and human rights impact assessments for AI systems. (Addresses the following recommendations from the draft framework 1.1, 2.2, 2.3, 3.2, 4.1, 4.2, 6.1, 6.2, 6.4, 6.12, 6.13, 10.2, 11.1 referenced in Appendix G.)

This recommendation calls for centralized privacy efforts led by a privacy leadership role to ensure ethical AI deployment through privacy-by-design principles and compliance with data privacy laws. Key tasks include formalizing the privacy leadership role, creating policies on informed consent, disclosure, opt-outs, and transparency, and conducting privacy and human rights impact assessments. By setting standards for data minimization, documentation, and privacy safeguards in AI systems, and aligning with Executive Branch programs, state government aims to protect privacy, build public trust, and institutionalize responsible AI practices.

Because privacy is intricately related to data activities, this recommendation also includes actions related to continuing agency data governance efforts. As with other agency data activities, consideration should be given to data of native and sovereign nations and the practice of data sovereignty. Oregon's Data Strategy and data governance acknowledge the importance of engaging communities and recognizing both community self-determination and indigenous and tribal data sovereignty as critical components of a mature data organization.

Privacy is essential to establishing trust, accountability, and equitable outcomes in AI. This recommendation calls for a centralized privacy framework—led by a privacy leadership role—to guide responsible, privacy-focused AI deployment across Oregon’s state government. By creating clear statutory authority, implementing privacy-by-design principles, and adhering to federal and state regulations, this framework safeguards personal data and fosters public trust. Through informed consent policies, routine privacy impact assessments, and close collaboration with Executive Branch programs, the state aims to institutionalize privacy-centered AI practices.

[7] https://www.govtech.com/biz/data/is-your-government-ai-ready-an-interactive-tracker-of-ai-action

Ultimately, these efforts provide a robust, adaptable foundation for transparent and people-centered AI.

Data governance is fundamental to responsible and effective AI, ensuring high-quality, accurate, and secure data throughout the AI lifecycle. By investing in continuing agency data governance and data quality efforts, this recommendation positions Oregon to better prepare for AI projects while upholding transparency, accountability, and ethical standards. Key steps include clarifying roles for agency data officers, crafting statutory language to support agency-level data governance, and integrating robust documentation requirements into procurement and project planning. Through collaboration among the State Chief Data Officer, privacy leadership role, and Executive Branch programs, Oregon can align data management with AI best practices—ultimately fostering public trust, promoting innovation, and delivering equitable outcomes for all Oregonians.

High level tasks and resources needs are provided in Appendix C.

Enhance security framework to include protocols to support recovery from disruptions and effectively manage AI-related incidents. Develop a risk management framework and policies for AI systems, prioritizing risks through an evidence-based approach with appropriate security controls. Update security incident response and disaster recovery framework and policies and procedures to account for AI technologies. (Addresses the following recommendations from the draft framework 2, 3, 3.3, 3.4, 6.3, 7.1, 7.3, 7.4, 7.7, 9, 9.2, 9.4, 9.5, 9.6, 12 referenced in Appendix G.)

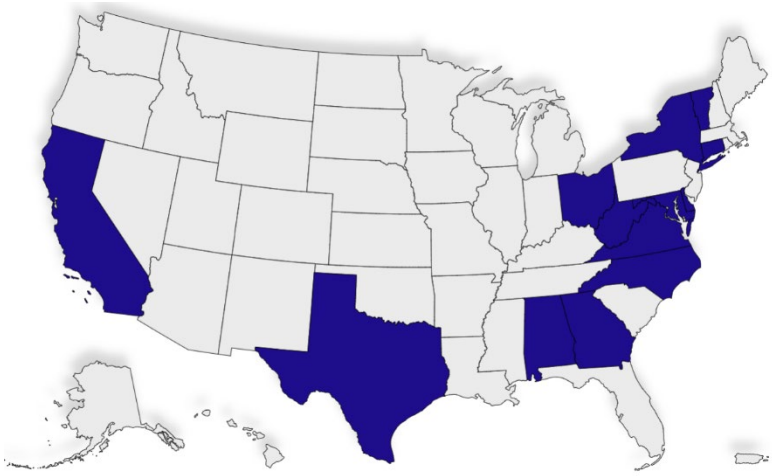
The purpose of this recommendation is to respond to incidents and restore normal operations for services and preserve quality and system availability. Incident management framework will focus on processes to identify and resolve the root causes of incidents and thus minimize the adverse impact of incidents that are caused by errors in systems that utilize AI.

A comprehensive security plan including well defined risk management practices, considerations for incident response, and integration with existing cyber and disaster recovery efforts helps to ensure AI systems function as intended.

High level tasks and resources needs are provided in Appendix D.

Develop reference architecture and policies for acquisitions, development, testing, and auditing of AI systems and use. (Addresses the following recommendations from the draft framework 3.1, 6.5-6.11, 7.2, 7.5, 7.6, 8.2, 8.3, 9.7, 11.3-11.5, 11.7, 11.8 referenced in Appendix G.)

Figure 3: States who have an AI inventory[8]



Baseline maturity activities for this recommendation include developing a state AI use case inventory or similar output to track AI activities across Executive Branch agencies. State use of AI will cover a broad spectrum of service delivery models. Each delivery model will necessitate specific safeguards to ensure responsible use. Generative AI experiences will depend heavily on resource access management and data loss prevention. Constituent focused conversational AI assistants built on commercially available large language models will require rigorous human validation to ensure accurate, consistent, and harm free responses. Decision support systems developed with AI components will require detailed documentation describing the training, testing, results, and validation steps taken to ensure accuracy and transparency.

A mature AI reference architecture will capture and communicate traditional layers describing data, development, deployment, operations, security and user experience. The reference architecture will also describe AI specific layers including specialized hardware necessary for model performance, ethics and explainability, integration, and AI audit and governance. Additionally, this will necessitate developing standard AI performance metrics including accuracy, robustness, inclusivity, and unintended biases.

The Executive Branch aims to implement AI across a range of service delivery models from curated generative AI experiences to decision support systems. To support this effort, a mature AI reference architecture will outline traditional layers (data, development, deployment, operations, security, user experience) and additional AI-specific layers (specialized hardware, ethics and explainability, integration, and AI audit/governance). These tasks will require new roles, interdisciplinary teams, ongoing training programs, and investments in staff and workforce development, technology and support and professional services.

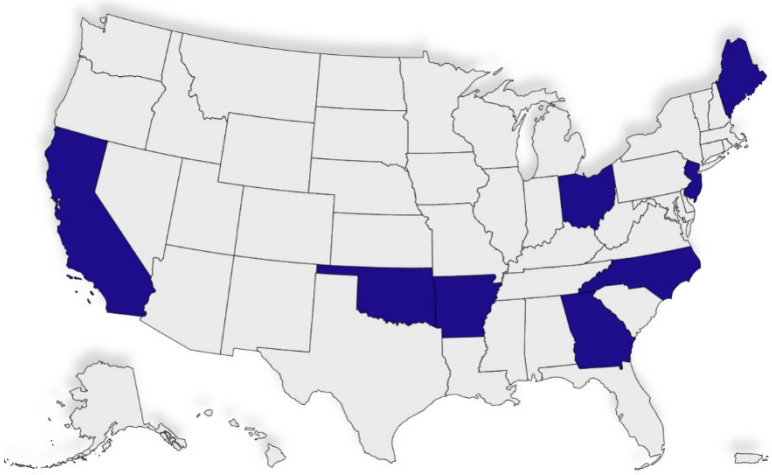
High level tasks and resources needs are provided in Appendix E.

[8] https://www.govtech.com/biz/data/is-your-government-ai-ready-an-interactive-tracker-of-ai-action

Address workforce needs recognizing the criticality of existing and future workforce. (Addresses the following recommendations from the draft framework 2.12, 4.3, 4.4, 12.1, 12.2, 12.3, 12.4, 12.5, 12.6 referenced in Appendix G.)

To echo Oregon's vision of developing an empowered and educated workforce around AI, the high-level tasks provided in Appendix F are vital to ensure state employees are part of the adoption and review process of AI technology and trained with the knowledge on how to leverage any AI tools that may be adopted. AI systems are intended to support worker efficiency, and Oregon's state workforce should be equipped to responsibly foster the AI ecosystem long term. The high-level tasks will contribute to state employees anticipating advancements made in the field of AI, will highlight the importance of their role when it comes to being the human-in-the-loop, carefully auditing automated tasks, and will help develop improved drafting of policy, with a focus on eliminating bias, and adding consideration for AI into modification of existing state business processes.

Figure 4: States who have AI training[9]



Oregon's workforce development strategy underscores the state's education to equipping employees for the evolving role of AI in government operations and readying future employees. Through investments in targeted training programs, the establishment of clear governance structures, and the development of critical technical infrastructure, the state is addressing both immediate and long-term workforce needs. Initiatives such as data literacy programs and specialized training in AI ethics are supported by a comprehensive resource framework that integrates dedicated staffing, advanced technological tools, and strategic external partnerships. This integrated approach, grounded in equity, privacy, and ethical principles, ensures Oregon's current and future workforce is not only technically skilled but also prepared to implement AI responsibly and inclusively across state agencies.

[9] https://www.govtech.com/biz/data/is-your-government-ai-ready-an-interactive-tracker-of-ai-action

High level tasks and resources needs are provided in Appendix F.

Concluding Summary

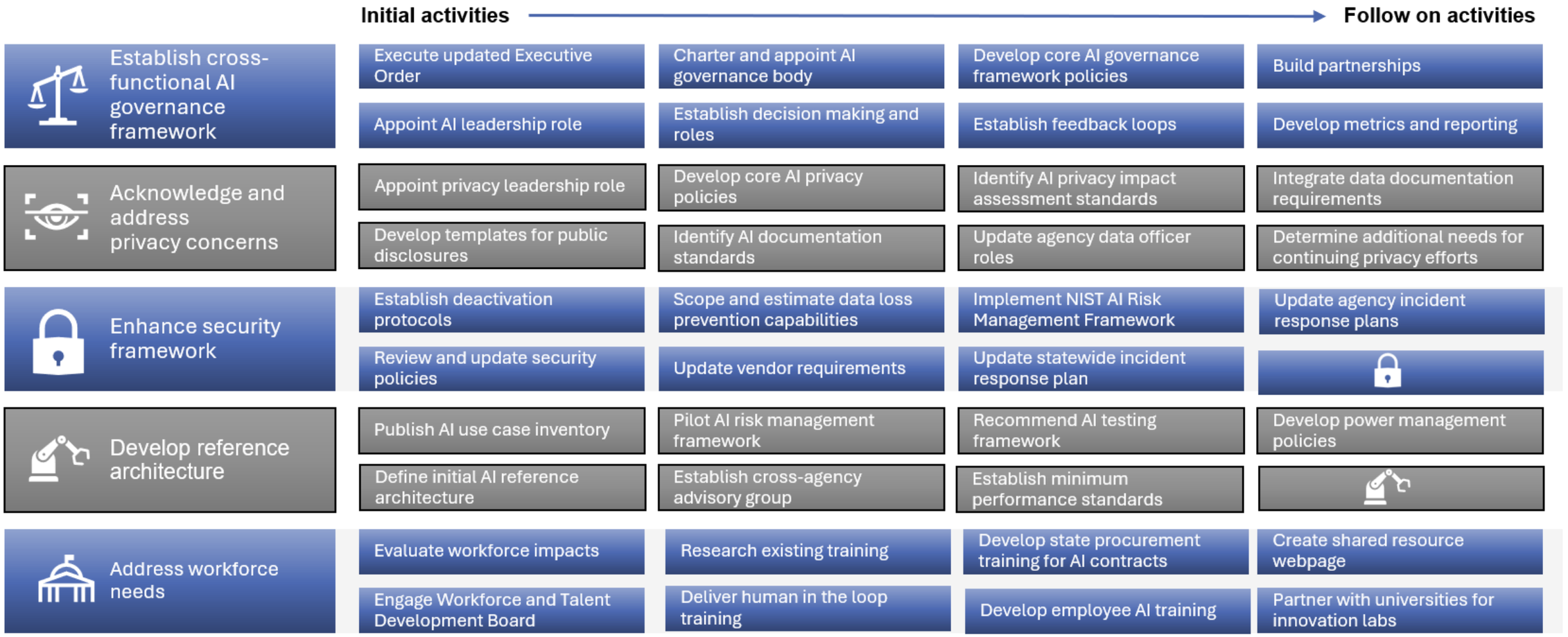
Through months of public meetings, subcommittee work, and stakeholder engagement, the AI Council developed a set of AI principles, a framework, and 74 recommendations for responsible AI adoption within Oregon state government. Building on these foundational elements, Enterprise Information Services staff created a comprehensive action plan that translates the Council's work into concrete initiatives, aligning with Oregon's core values of diversity, equity, and inclusion. By establishing robust governance structures, enhancing privacy and security measures, and investing in workforce readiness, the plan positions Oregon to navigate AI's complexities with transparency and accountability. In doing so, Oregon stands poised to harness AI's transformative potential for the benefit of all Oregonians. The 74 recommendations are presented in an Appendix to this plan so that their intent remains concrete, and they can be referenced for additional context and detail as the action plan is utilized.

The guiding principles are visionary and foundational for ongoing and future actions. Actions in the plan are designed to be immediate and short term with the anticipation that they will be enhanced and augmented as they are fulfilled. The resources and timeframes estimated align with the immediate and short-term actions. Actions will need to be further elaborated and prioritized in an implementation plan as existing resources will not be able to perform all actions simultaneously.

It is fully expected that subsequent actions will be identified and defined along with associated resources identified and requested. To formalize an updated estimate of needed resources, the AI leadership role and the privacy leadership role should plan to provide a progress report to support the 2027-29 budget development process.

The State Chief Information Officer appreciates the opportunity to chair the State Government Artificial Intelligence Advisory Council and endorses this report.

Appendix A: Recommended Action Plan High Level Roadmap



*NIST: National Institute of Technology and Standards

Appendix B: Establish cross-functional AI governance framework: Tasks and estimated needs

The following high level tasks should always be fully guided and informed by Oregon's Artificial Intelligence Guiding Principles (pp. 4-5).

High level tasks:

1. Execute an updated Executive Order authorizing AI Governance Body. (Governor; 6 months)
2. Appoint an AI leadership role. (State Chief Information Officer; 6 months)
3. Charter and appoint an AI governance body with membership to include advocates, subject-matter experts, front line workers, and representatives from historically underrepresented communities. (AI leadership role; 6 months)
4. Convene an AI governance body to establish clear, transparent, decision-making processes, roles, partnerships, metrics and reporting. Processes will recognize varying needs between building AI systems, fine tuning AI systems and deploying AI systems. (AI leadership role; 6 months)
5. Build partnerships and foster collaboration with various stakeholders by hosting webspace to encourage sharing of knowledge, resources, and best practices. (AI leadership role; 6 months)
6. Engagement with Governor's Tribal Affairs Director on addressing tribal data sovereignty as part of the state's tribal engagement policy. (Chief Data Officer; 6 months)
7. Develop core AI governance framework policies integrated with existing project management, procurement, development, oversight, and compliance systems.
    7.1. AI-assisted decision approval chain policy to document decision-making processes, the risk and criticality level of the AI-assisted decision being rendered and acknowledgement of explicit accountability roles regarding AI systems. (AI leadership role; 12 months)
    7.2. Human oversight policy that requires human review for critical steps and sign-off for predefined high-risk AI use cases (e.g., those impacting civil rights, access to public safety, adverse employment decisions, or access to social safety net benefits or assistance). (AI leadership role; 12 months)
    7.3. Validation policy regarding the frequency and content of periodic audits to ensure human oversight remains effective. Policy will consider risk level. (AI leadership role; 12 months)
    7.4. AI Evaluation Checklist Policy to include detailed criteria for ethical data sourcing, thorough bias assessments, sampling justifications, and evidence of compliance with relevant regulations and standards. (AI leadership role; 12 months)
    7.5. Equity impact assessments policy with standardized templates to identify and mitigate biases, documenting equity considerations (Cultural Change Officer; 12 months)
    7.6. Recommend policy to evaluate and guide decisions of AI use that could result in undesirable environmental and global impacts. (AI leadership role; 12 months)
8. Establish feedback loops to address concerns and observations regarding AI safety and security and AI initiatives currently underway. Review and integrate feedback into decision-making processes, focusing on concerns related to fairness, equity, and representation. (AI leadership role; 12 months)
9. Develop metrics, measure and report publicly. (AI leadership role; 18 months)

9.1. Develop metrics to measure progress in addressing biases, improving representation in datasets, and ensuring that system outputs equitably serve all populations.
9.2. Conduct periodic equity audits to verify compliance, highlight best practices, and identify areas for improvement.
9.3. Release an annual public report on AI usage, metrics, and related information.

Resource and investment needs estimated:

Staffing

1. AI leadership role (position authority and funding) to oversee policy formation, enforcement, and inter-agency coordination.
2. Governance body members (volunteers).
3. Two AI governance staff (2 FTE position authority and funding) to initiate the program. As the programs matures, the AI leadership role will estimate future needs.

Technology

1. Tools capable of performing bias detection and fairness analyses on datasets and algorithms.

Support Services

1. Department of Justice legal consultation to confirm framework tools align with current laws and regulations.
2. External consultants or academic partners who specialize in equitable AI design, fairness metrics, and community engagement strategies.

Appendix C: Acknowledge and address privacy concerns: Tasks and estimated needs

The following high level tasks should always be fully guided and informed by Oregon's Artificial Intelligence Guiding Principles (pp. 4-5).

High level tasks:

1. Appoint a privacy leadership role. (State Chief Information Officer; 6 months)
2. Develop a checklist to help Executive Branch agencies classify AI use cases as "high-risk," "low-risk," or "prohibited" based on privacy and data considerations. (privacy leadership role; 6 months)
3. Develop templates for informed consent, opt-outs options, appeals processes, transparency, data minimization and public disclosures tailored to individual agency needs, supported by enterprise guidance. Guidance will evaluate the level of impact of decision making. (privacy leadership role; 12 months)
4. Create detailed policies and technical guidelines (policies and guidelines will clarify data used by AI systems and data used to train AI systems):
    a. Data documentation requirements for AI projects, addressing ethical and performance considerations (privacy leadership role; 6 months)
    b. Data documentation policy for AI solutions, defining specific criteria for requirements and decisions of AI systems procurements, project management and performance management. (Chief Data Officer; 6 months)
    c. Data quality and AI readiness checklists for data in preparation and planning for AI projects. (Chief Data Officer; 12 months)
    d. AI implementation, including standards for privacy impact assessments, data privacy documentation, and risk categorization. (privacy leadership role; 18 months)
    e. Preventing state government AI systems from generating content that violates data privacy laws. (privacy leadership role; 18 months)
    f. Prohibiting the collection, storage, or use of sensitive information in any interactions involving large language models (LLMs) or generative AI systems. These guidelines should ensure data minimization and protect privacy throughout the lifecycle of AI systems. (privacy leadership role; 18 months)
    g. Align AI development and use with applicable data privacy laws and regulations, including those related to data privacy, copyright and intellectual property law. (privacy leadership role; 18 months)
    h. Initiate a statewide privacy framework to institutionalize privacy-by-design principles in all AI procurement, development, and deployment projects to incorporate privacy considerations from the outset, including strict adherence to data minimization, secure processing, and documentation standards. (privacy leadership role; 24 months)
5. Identify documentation and privacy impact assessment standards for AI solutions to create transparency around training data and privacy impacts. (privacy leadership role; 24 months)
6. Update roles and responsibilities for agency data officers and clarify agency expectations for data governance. (Chief Data Officer; 12 months)

7. Incorporate specific criteria for requirements and decisions of AI system procurements and contracts, (e.g. data documentation requirements). (State Chief Procurement Officer; 18 months).
8. Determine future needs for continuation of privacy framework efforts. (privacy leadership role; 18 months)

Resource/Investment Needs:
Staffing

1. Privacy leadership role (position authority and funding).
2. Privacy Analysts (2 FTE position authority and funding) to support enterprise privacy efforts, with one Privacy Analyst dedicated to AI-specific privacy considerations. This is an estimate for initiating privacy efforts. After initiation, the privacy leadership role will be able to articulate appropriate staffing needs to manage efforts for longevity.
3. Executive Branch FTE needs of individuals agencies for ongoing data governance and privacy compliance have not been estimated.

Technology

1. Ongoing resourcing, software and technical needs will be identified by the privacy leadership role as part of ongoing privacy efforts.

Support Services

1. Consulting services to support development of enterprise privacy practices.
2. Department of Justice legal consultation for advice, evaluation, compliance.

Appendix D: Enhance security framework: Tasks and estimated needs

The following high level tasks should always be fully guided and informed by Oregon's Artificial Intelligence Guiding Principles (pp. 4-5).

High level tasks:

1. Establish protocols to ensure AI systems can be deactivated when necessary. (AI leadership role; 6 months)
2. Review and update security policies to address AI considerations. (Chief Information Security Officer; 12 months)
3. Scope and estimate data loss prevention operations capability. (Chief Information Security Officer, 12 months)
4. Implement the National Institute of Standards and Technology Artificial Intelligence Risk Management Framework (AI RMF 1.0). (AI leadership role; 12 months)
5. Review and update statewide incident response plan for AI technologies, while aligning with relevant breach reporting, data protection, data privacy, and other laws. Provide guidance for agencies plan updates. (Chief Information Security Officer, 12 months)
6. Review and update existing vendor contract templates and service level agreements that specify content ownership, usage rights, quality standards, security requirements, disclosure requirements, and content provenance expectations for AI systems. (State Chief Procurement Officer; 18 months)

Resource/Investment Needs:

Staffing

1. State Procurement Services (1 FTE position authority and funding).
2. Executive Branch agencies' FTE needs for updating agency incident plans and related activities have not been estimated.

Technology

1. Data analytics and security monitoring tools capable of detecting anomalies or breaches related to AI-driven systems.

Appendix E: Develop reference architecture: Tasks and estimated needs

The following high level tasks should always be fully guided and informed by Oregon's Artificial Intelligence Guiding Principles (pp. 4-5).

High level tasks:

1. Publish statewide AI use case inventory with accompanying deployment documentation. (Chief Technology Officer; 6 months)
2. Define high level AI reference architecture with evaluation and approval process (Chief Technology Officer; 12 months)
3. Establish cross-agency advisory group - a small, voluntary working group from existing personnel to compare risk assessment experiences, share best practices, and refine processes for broader implementation. (AI leadership role; 12 months)
4. Recommend an AI testing capability and framework. (AI leadership role; 12 months)
5. Establish minimum thresholds for performance or assurance criteria and review as part of deployment approval (policies, procedures, and processes, with reviewed processes and approval thresholds reflecting measurement of AI capabilities and risks). (AI leadership role; 12 months)
6. Develop policies that include power management protocols and server shutdown processes to prevent resource overuse from local generative AI applications. (Data Center Services Director, 12 months)
7. Pilot AI Risk Management Frameworks. Test structured risk management tools or lightweight frameworks (potentially adapted from NIST's AI RMF) on select AI initiatives before wider adoption. (AI leadership role; 18 months)

Resource/Investment Needs:

Staffing

1. AI Architect (position authority and funding)

Support Services

1. Management of locally hosted AI models, particularly generative AI and large language models, requires specialized expertise. To support this capability, it is recommended that subject matter experts in AI technologies be recruited. These roles would address the unique demands of the specialized hardware and software associated with these models, which are not currently within Data Center Services' expertise.
2. AI Architecture Training, professional services for development of a comprehensive AI reference architecture

Appendix F: Address workforce needs: Tasks and estimated needs

The following high level tasks should always be fully guided and informed by Oregon's Artificial Intelligence Guiding Principles (pp. 4-5).

High level tasks:

1. Engagement with Oregon Workforce and Talent Development Board to help prepare current and future workforce and work in consultation with key labor and employment stakeholders. (AI leadership role; 6 Months)
2. Create shared resource pool/page for community awareness. (AI leadership role; 6 months)
3. Research existing AI training/development certification programs and/or standards. (Chief Technology Officer; 6 Months)
4. Consultant led training session for agency leaders and staff about privacy in AI, including privacy impact assessments, regulatory compliance, and risk mitigation strategies. (privacy leadership role; 12 months)
5. Evaluate workforce impacts. (Chief Human Resource Officer; 12 months)
6. Determine training availability, certification body, and if the state will manage or centralize record of training. (AI leadership role; 12 months)
7. Deliver human in the loop training. (AI leadership role; 18 months)
8. Ongoing training support from experts in privacy law and ethical AI to ensure staff remain current on evolving data protection trends. (privacy leadership role; 18 months)
9. Offer basic training for development teams and decision-makers on recognizing, measuring, and addressing biases in AI systems, leveraging internal staff or free educational resources. (AI leadership role; 18 months)
10. Develop state procurement trainings for AI specific contracting language. (State Chief Procurement Officer; 18 months)
11. Develop scenario testing and simulation to allow human in the loop reviewers and decision-makers to practice responding to edge cases, emergent ethical dilemmas, or system anomalies, continuously honing their judgment and response protocols. (AI leadership role; 18 months)
12. Scope, develop and expand comprehensive training programs with academic and industry partners to equip state employees and local jurisdictions with skills and knowledge on equitable AI practices and emerging technologies. (AI leadership role; 24 months)
13. Establish innovation labs in collaboration with universities and industry to pilot AI solutions addressing public challenges, including those involving AI governance, and equitable AI practices. At the same time, readying a future workforce. (AI leadership role; 24 months)

Resource/Investment Needs:

Staffing

1. AI training coordinator (position authority and funding)
2. State Procurement Services trainer (position authority and funding)

Technology

1. Virtual lab environments for hands-on practice, simulating real-world AI use cases and security scenarios.

Support Services

1. Ongoing consultation on curriculum standards, skill assessment models, and emerging technologies.
2. Academic partnerships to develop accredited courses and provide expert guest instructors.
3. Department of Justice legal consultation for advice, evaluation, compliance.
4. Organizational change management consultants to help design participatory governance models and facilitate constructive dialogue between management, staff, and other stakeholders.

Appendix G: Framework Recommendations

The AI Council Recommended Plan and Framework identifies recommended 74 individual recommendations to support Oregon in upholding its AI guiding principles. The final recommended action plan summarizes these 74 recommended into executive action along with estimated resources needs and timeframe. To facilitate effective use of the action plan, the detailed recommendations are provided in this appendix for continual reference and adherence.

1. Accountability

Operational Policy and Guidelines

1.1 Develop parameters for the IT department for metrics and criteria for evaluation, mechanism, and timelines for review. Regulatory and Governance

1.2 Establish clear, transparent, decision-making processes and roles (key endorser, final stamp of approval).

2. Equity and Representation

Collaboration and Partnerships

2.1 Identify opportunities for public-private partnerships, public-academic partnerships, or similar collaboratives with organizations and private companies committed to equitable AI development and technology for the public good.

Data Governance and Management

2.2 Ensuring that data development and AI development are in alignment with Oregon's Data Strategy principles.

2.3 Oversight measures and expectations for agencies will include expectations for documenting data representation, visibility, and quality and avoid discrimination and replication of systemic harm(s).

Methodology and Testing

2.4 Establish methods and requirements in the AI development lifecycle that ensure equity, representation, and inclusion are considered crucial components of development, rather than "checklist" items.

2.5 Set standards and guidelines for agencies to evaluate and embed awareness of biases and inaccuracies into AI development.

Policy Alignment and Development

2.6 AI accountability, governance, and oversight structures should embody the state's values of diversity, equity, inclusion, and belonging in how they are developed, implemented, and overseen. Measurement of agency compliance should be balanced with investment in developing agency capacity to mature their AI governance structures.

2.7 Develop and implement an AI governance framework that incorporates principles of diversity, equity, and inclusion as foundational elements in partnership and consultation with communities and community partners. This framework should guide AI system development and deployment to ensure that AI solutions reflect the diverse needs and values of our constituents.

2.8 Establish requirements and expectations for agencies that include direct community engagement to gather input from affected populations in AI system development, procurement, and deployment. Requirements should include acknowledgement that community engagement be an ongoing process, not just a one-time consultation.

Regulatory and Governance

2.9 Define expectations of how agencies uphold demonstration of protecting human rights and inclusion.

2.10 Establish a responsible body/authority to oversee, govern, ensure adherence to principles and to craft appropriate governance structures to support.

2.11 Establish and resource an appropriate position and authority to set the state's AI governance and oversight structure and model, that includes requirements and expectations for how state agencies will engage with the AI oversight office/role.

2.12 Identify resource and capacity gaps affecting agency compliance with AI oversight and governance.

2.13 Include a community advisory body or other community-engaged oversight into statewide AI governance. Community advisory body should have a role in reviewing agency equity impact assessments or other tools for evaluating equity within AI solutions.

3. Explainability and Trust

Operational Policy and Guidelines

3.1 Develop processes, guidelines, and procedures for Oregonians interfacing with any AI system to do so with informed consent. Establish and make transparent an opt-out and/or appeals process for decisions made by an AI system. Regulatory and Governance

3.2 Adopt performance metrics to build trust and track accuracy. Develop adoption processes where key metrics must be achieved and weighed against any negatives or costs. Develop reevaluation processes where key metrics must be achieved, weighed against any negatives or costs for system use to continue.

3.3 Develop and make publicly available a statewide AI use case inventory, with an expectation that further documentation on deployment will be provided.

3.4 Produce and make public an annual report on use, metrics, etc.

4. Governance

Methodology and Testing

4.1 Develop metrics for measuring AI performance, including accuracy, robustness, and unintended biases. Regularly assess the effectiveness of risk controls and adjust as needed.

4.2 Develop policy and standards to ensure adherence to laws, regulations, and guidelines specific to AI and data management, including specific documentation, mapping, reporting, auditing, and information disclosure.

Operational Policy and Guidelines

4.3 Build workforce expertise by investing in AI-specific training and development programs that establish and maintain skilled, vetted, and diverse service verticals in the AI workforce.

4.4 Develop a comprehensive AI security training and certification program, including clear training plans, requirements, and a certification process for AI users.

Regulatory and Governance

4.5 Create and maintain a chartered governance body or council to oversee AI practices.

4.6 Establish clear, transparent, decision-making process and roles (key endorser, final stamp of approval).

4.7 Perform periodic reviews and refinement of governance activities.

5. Human Oversight in AI Governance

Regulatory and Governance

5.1 Ensure human-in-the-loop (HITL) oversight in the adoption and deployment of AI and decision-making systems.

6. Privacy and Confidentiality

Data Governance and Management

6.1 Policies, guidelines, and expectations for AI implementation should promote data minimization and other privacy protection strategies in AI system design to limit the amount of data collected and processed, reducing potential privacy risks.

Methodology and Testing

6.2 Guidance and support for incorporating privacy considerations into AI development and deployment, including data documentation and privacy impact assessments, should describe the nature of data in use, identify personal or sensitive fields, and address restricted or sensitive data.

Operational Policy and Guidelines

6.3 Develop and implement incident response procedures specifically for AI systems. These procedures should address the disclosure or breach of confidential data, notification requirements, and remediation approaches consistent with existing state privacy and breach notification laws and procedures.

6.4 Offer implementation guidance around “high risk”, “low risk” or “prohibited” uses of AI tools as they apply within Oregon (sample language from organizations like the European Union might be possible) to assist agencies in evaluating use cases associated with AI.

6.5 Policies, guidelines, and expectations for state agencies and employees shall prohibit the use of confidential data in public AI models.

Procurement

6.6 Agency contracts shall prohibit the use of confidential data in public AI models.

6.7 Agency contracts shall prohibit vendors from using Oregon materials or data in generative AI queries, or for training proprietary models unless explicitly approved by the state.

6.8 Agency contracts shall require vendors to adhere to strict data use standards, ensuring that government-provided data is used exclusively for government purposes and serves as a non-negotiable clause in contracts.

6.9 Examine existing state contracting language to ensure vendors are compliant with all necessary state and federal privacy laws and regulations and to incorporate privacy compliance into assessments during the procurement process.

6.10 Require change management processes for vendors be documented so that state agencies are informed of any changes to AI systems, especially large language models, regardless of perceived impact, to ensure state agencies can proactively manage impacts on service delivery or implementation.

6.11 Wherever possible, vendors should be required to disclose datasets used to train AI models during the procurement process. Disclosures should be made public where applicable and incorporated into state procurement processes and expectations for AI systems.

Regulatory and Governance

6.12 Engage public privacy programs to ensure alignment in protecting privacy within Oregon AI systems.

6.13 Establish a centralized privacy program with leadership and resources to conduct privacy impact assessments and human rights impact assessments for AI systems. This program should ensure that AI initiatives comply with federal, state, and other relevant privacy laws.

7. Risk and Risk Management

Methodology and Testing

7.1 Assess and track the performance of risk controls and mitigations in addressing the specific AI risks identified in the mapped data types.

7.2 Develop and promote behaviors of AI risk management by aligning AI safety and security with organizational principles.

7.3 Establish and deploy a risk management framework and methods.

7.4 Establish risk mitigation methodologies that reduce risk.

7.5 Implement continuous testing and auditing of AI systems to detect errors, vulnerabilities, and other risks. Use dedicated environments for testing to prevent exposure of sensitive information.

Regulatory and Governance

7.6 Conduct thorough AI impact assessments as part of the deployment or acquisition process, documenting the intended purposes, and expected benefits.

7.7 Prioritize AI risks using an evidence-based approach, applying appropriate security controls.

8. Safety and Impact

Collaboration and Partnerships

8.1 Establish feedback loops with stakeholders to report and receive input on AI safety and security, ensuring that all concerns are addressed promptly.

Methodology and Testing

8.2 AI design must be tested against AI safety standards.

Operational Policy and Guidelines

8.3 Risk impact assessment is completed prior to deployment in production.

9. Security and Securing

Methodology and Testing

9.1 Continuously monitor and document AI risks, including those specific to attacks using AI, attacks on AI, and AI design failures. Regularly update risk controls or mitigations as new threats emerge.

9.2 Establish capability and enforce data loss prevention and provide for continuous monitoring.

9.3 Establish reference architecture for approved AI models and deployments.

9.4 Establish 'secure by design' practices throughout the AI lifecycle.

9.5 Monitor AI system behavior continuously for signs of anomalies or malicious activities.

Operational Policy and Guidelines

9.6 Maintain an incident response plan that includes AI based service implementations, ensuring recovery from disruptions and clear protocols for addressing AI-related incidents.

Procurement

9.7 Establish processes to review AI vendor supply chains for security risks, ensuring that all hardware, software, and infrastructure meet security and safety standards.

Regulatory and Governance

9.8 Conduct thorough AI impact assessments as part of the deployment for potential safety and security risks.

10. Stakeholder Experience and Equity

Policy Alignment and Development

10.1 Develop a checklist of must-haves in evaluating and adopting any system. Items should include proof of ethical sourcing of data, evaluation of potential discrimination bias of the data, and documentation on reasoning of sampling.

10.2 Develop evaluation systems and metrics to ensure that programs promote inclusivity and actively work to not perpetuate negative outcomes or biases for currently or historically marginalized people, including Oregonians interfacing with the system and workers across the globe enabling these systems to function and consider any negative environmental systems.

11. Transparency and Trustworthiness

Collaboration and Partnerships

11.1 Develop or invest in third party audit/oversight capabilities for external partners to conduct AI system reviews.

11.2 Foster collaboration and build partnerships with various stakeholders, including industry, academia, government agencies, local jurisdictions, and other public body partners. Encourage sharing of knowledge, resources, and best practices to enhance AI development and deployment.

Methodology and Testing

11.3 Implement standardized continuous testing and auditing processes for deployed AI solutions to protect against bias, monitor system performance, and ensure systems are meeting intended outcomes. These processes should be developed in partnership with state agencies and standardized to maintain consistency.

Procurement

11.4 Develop policies requiring AI systems to be compliant with public records laws, even if AI-generated content is not initially subject to such laws, to create further transparency around how to respond to and navigate public records requests related to AI systems. Set expectations for vendor transparency in system development and design to be compliant with state public records laws and data transparency and interoperability requirements.

11.5 Set forth expectations for vendors in support of complying with transparency and trustworthiness when bidding for AI contracts. Explore requirements around transparency and trustworthiness for vendors.

Regulatory and Governance

11.6 Ensure that AI systems incorporate human oversight, especially in areas impacting equity and ethics. This approach ensures that AI systems are accountable and aligned with the state's

values, and support development of AI systems as a tool to support worker efficiency, not to replace human decision-making.

11.7 People should know when and how they are engaging with AI.

11.8 Set expectations of mandatory public disclosure when GenAI or similar AI capabilities are used in processes to produce a decision.

12. Workforce Preparedness and Understanding

Collaboration and Partnerships

12.1 Explore partnerships with academia to build training curriculum to help ensure that the future generation of workers have a baseline of AI education – including what is possible with AI, ethical considerations and implications, and direct and practical applications.

12.2 Make available state trainings, materials, and resources to the general public.

12.3 Submit/engage Oregon's Workforce and Talent Development Board on any recommendations.

Data Governance and Management

12.4 Develop and implement informed worker consent on AI use and for how and when their data is being collected and used.

Operational Policy and Guidelines

12.5 Provide general training for all workers, and certification process/more specific training for those directly using any AI platforms.

Regulatory and Governance

12.6 Develop and implement a process for including front-line (i.e. those actually using the system) workers in conversations and decisions about the adoption, implementation, and ongoing evaluations of AI platforms. Establish and make transparent an opt-out and/or appeals process for decisions made by an AI system.

Appendix H: AI Advisory Council Membership

The State Chief Information Officer would like to recognize the Council that offered their time and talents toward the completion of this recommended action plan and related components.

Name	Title
Terrence Woods	State Chief Information Officer
Kathryn Darnall Helms	State Chief Data Officer
Melinda Gross	Department of Administrative Services Cultural Change Officer
Daniel Bonham	Member of the Oregon State Senate
Daniel Nguyen	Member of the House of Representatives
Jesse Hyatt	Executive Branch Agency Representative
Andres Lopez	Member
Catie Theisen	Member
Hector Dominguez Aguirre	Member
Janice Lee	Member
Justus Eaglesmith	Member
Ellen Flint	Member
K S Venkatraman	Member
Saby Waraich	Member