2025

LESSONS & RECOMMENDATIONS

Responsible AI in the Public Sector

How the Washington State Government Uses & Governs Artificial Intelligence

WaTech
Washington Technology Solutions

CITRIS THE BANATAO INSTITUTE | CITRIS POLICY LAB

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Table of Contents

Authors **1**
Acknowledgments **1**
Executive Summary **2**
Navigating the Report **2**
Introduction **3**
Use of AI in the Public Sector and the Need for Governance and Oversight 3
What is AI? What Kinds of AI are in Scope for this Report? 3
Section 1. Recommendations for WaTech **5**
Section 2. Washington State Case Study **9**
Overview of Washington's AI Governance Efforts 9
Executive Order 24-01 and Generative AI (GenAI)-Specific Efforts 10
The WaTech-Berkeley Collaboration 13
Interview Findings and Insights 13
Survey Results and Insights 17
Section 3. Existing and Potential Applications of AI Within the Public Sector **26**
The Use of AI within the Public Sector: Introduction 26
Overview of AI in the Public Sector: A Brief History 26
Types of AI Technologies and Tools in the Public Sector 26
Section 4. Opportunities & Barriers to AI Adoption **31**
Section 5. Responsible AI Governance Strategies & Best Practices **33**
Understanding Responsible AI: Key Principles 33
Managing Risks: Strategies for Addressing Constraints and Risks 33
Aligning AI Governance with Values 36
Section 6. Strategies to Enable Responsible Public Sector AI Governance & Use **36**
Federal AI Governance Strategies 36
State-Level AI Governance Strategies 39
Section 7. Strategic Roadmap for AI Implementation & Oversight **42**
Short-Term Goals (6 months) 42
Medium-Term Goals (1-2 years) 43
Long-Term Vision (2+ years) 43
Appendix A. Methodology **45**
Appendix B. Survey Questions **45**
Appendix C. Results Summary **48**
Appendix D. Figures **49**

Authors

Brandie Nonnecke, Director, CITRIS Policy Lab & Assoc. Adjunct Professor, Goldman School of Public Policy, UC Berkeley
Jessica Newman, Director, AI Security Initiative, Center for Long-Term Cybersecurity, UC Berkeley
Shannon Pierson, Senior Fellow, Public Interest Cybersecurity Program, Center for Long-Term Cybersecurity, UC Berkeley

Acknowledgments

We are grateful for the expert guidance received from State of Washington personnel, AI experts, state officials, and other partners involved in the support of this project and the drafting of the report. We want to thank the many individuals who participated in in-depth interviews, a roundtable discussion, and provided detailed survey responses. We are deeply grateful to the team at WaTech, including Nick Stowe, Katy Ruckle, Chaney Curry, Matt King, James Galvin, Hemingway Huynh, Tavares Terry, Cherry Quick, Angela Kleis, and Bill Kehoe for their invaluable partnership.

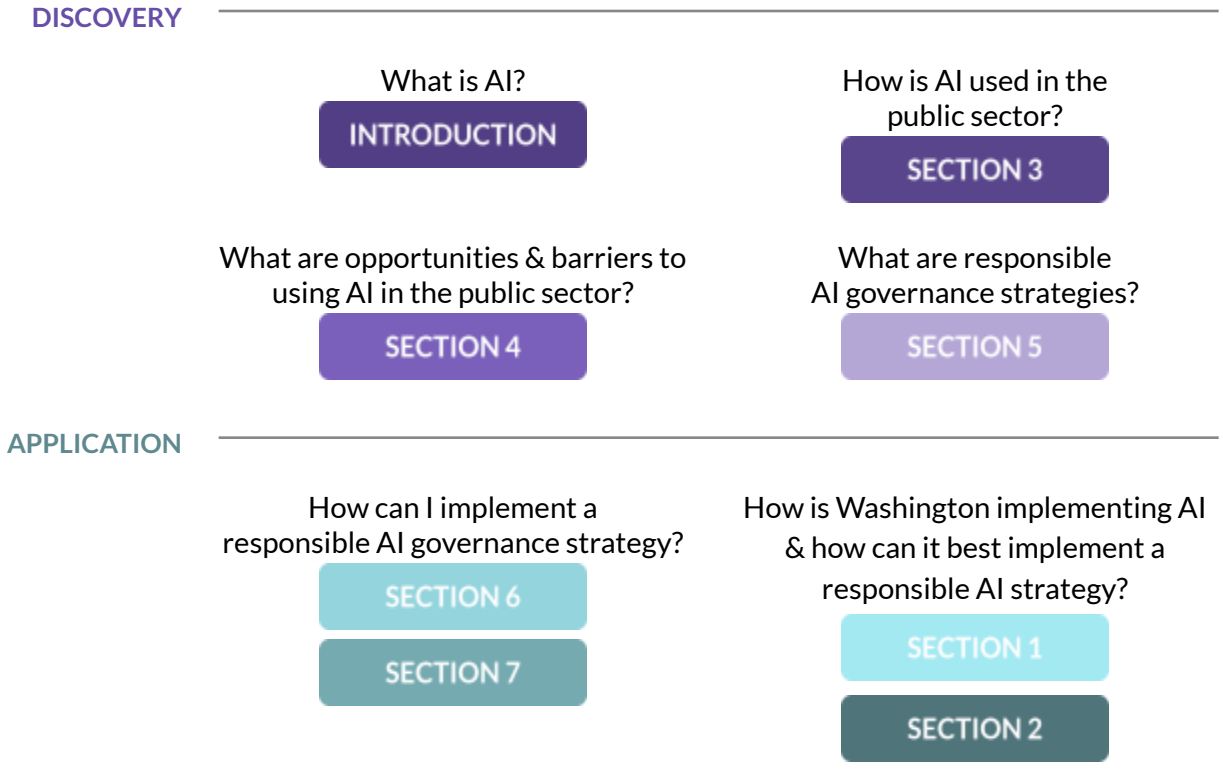
Image Credit

All images are royalty free from Pexels.com

Executive Summary

Washington Technology Solutions (WaTech) and the CITRIS Policy Lab and Center for Long-Term Cybersecurity at the University of California, Berkeley (UC Berkeley) worked in partnership throughout 2024-2025 to collaborate in support of Washington State's artificial intelligence (AI) governance efforts. This report is informed by that partnership, including regular engagement in Washington's AI Community of Practice and other fora, in-depth interviews, a roundtable discussion, and a survey distributed to Washington State and local government representatives. The report includes a case study of how Washington State is using and governing AI technologies, drawing upon the insights from the interviews and survey results. These insights include reasons for disparate patterns of AI use across agencies, particular areas where further policy clarity is desired, and ideas about how to better support public transparency and government accountability. The case study includes a list of 7 recommendations tailored to WaTech. The report additionally provides background and examples of how AI is being used throughout the public sector, discusses opportunities and barriers to AI adoption in the public sector, and highlights responsible AI governance strategies and best practices. Finally, the report discusses existing federal and state-level AI governance approaches to government use of AI, and lays out a strategic roadmap for AI implementation and oversight that can be broadly adopted throughout the public sector.

Navigating the Report



Introduction

Use of AI in the Public Sector and the Need for Governance and Oversight

The public sector is increasingly turning to artificial intelligence (AI) to enhance efficiency, improve service delivery, and manage vast amounts of data. From predicting resource needs to optimizing healthcare systems and automating administrative tasks, AI has the potential to significantly transform how governments operate. These advancements allow governments to address complex challenges with innovative solutions, enhancing decision-making and responsiveness. However, the rapid growth of AI technologies also comes with risks, especially when deployed in high-stakes environments such as law enforcement, public benefits administration, or critical infrastructure management. The promise of AI in the public sector is vast, but it necessitates robust governance frameworks that ensure fairness, transparency, and accountability.

Oversight of AI systems—from basic machine learning algorithms to advanced frontier models and generative AI (genAI)—has become increasingly critical in the public sector. These systems are often tasked with decisions that directly affect residents' lives, including eligibility for social services, judicial sentencing recommendations, and fraud detection. Without proper oversight, AI systems can perpetuate or exacerbate existing biases, make erroneous decisions, and operate without sufficient transparency, eroding public trust. Particularly as AI systems grow in complexity and their potential impact deepens, it is essential for governments to establish rigorous standards for their development and deployment. Oversight mechanisms such as algorithmic audits, accountability standards, and the development of responsible AI governance frameworks are crucial in safeguarding the public against unintended consequences. Effective governance ensures that AI serves as a tool for public good, reinforcing the principles of equity, fairness, and human rights that are foundational to public sector services.

What is AI? What Kinds of AI are in Scope for this Report?

Numerous definitions of AI have been proposed by governments and intergovernmental organizations. One prominent definition adopted by many governments globally comes from the Organisation for Economic Co-operation and Development (OECD):

> An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

The state of California has defined artificial intelligence similarly as "an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments."[1] The state of Washington has defined artificial intelligence as "A technology module or service that is built, integrated, or implemented in order to assist with or fully determine predictions, recommendations or decisions."[2]

In this report, we use AI as an umbrella term to refer to a range of different AI technologies, including primarily machine learning and generative AI. Importantly, we do not limit the scope of the report to genAI, despite the surge in interest across state governments over the last two years. Earlier AI technologies, including more simple machine learning architectures, have had a profound impact on state governments and residents and must not be ignored.

Many AI companies are also already shifting their focus away from genAI toward agentic AI (AI agents). AI agents, sometimes also referred to as advanced AI assistants, are designed to perform tasks in service of human goals, but without direct human intervention.[3] Companies are already using AI agents to carry out tasks such as booking meetings and responding to customers,[4] and state governments are likely to hear more about public sector uses too, despite numerous unresolved ethical challenges including safety, privacy, and influence.[5]

[1] AB 2885, Bauer-Kahan. Artificial intelligence, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB2885
[2] WaTech, 2024, Definition of Terms Used in Policies and Reports, https://watech.wa.gov/policies/definition-terms-used-policies-and-reports
[3] Navigating the AI Frontier: A Primer on the Evolution and Impact of AI Agents, https://www.weforum.org/publications/navigating-the-ai-frontier-a-primer-on-the-evolution-and-impact-of-ai-agents/
[4] Salesforce, Agentforce, https://www.salesforce.com/agentforce/
[5] Gabriel et al., The Ethics of Advanced AI Assistants, https://arxiv.org/pdf/2404.16244

Types of AI Addressed in this Report

Machine learning is an AI subfield concerned with the development and study of statistical algorithms that can learn from data without explicit instructions. Machine learning include:

- Supervised learning
- Unsupervised learning
- Reinforcement learning

Examples
Machine learning approaches facilitate descriptive and predictive analytics, which are used to interpret an organization's historical data either to identify patterns and trends or to make predictions about the future. These tools are widely used in the public sector, for example to support fraud detection.

Generative AI (genAI) is a technology that can create content, including text, images, audio, or video, when prompted by a user. GenAI systems learn patterns and relationships from large amounts of data, which enables systems to generate new content that may be similar, but not identical, to the underlying training data.

Examples
GenAI tools include large language models and AI chatbots that can generate high quality text in conversation with users. They also include tools that generate code, which can significantly help developers, as well as images, audio, and video, merely from natural language prompts.

Section 1. Recommendations for WaTech

The case study and interview and survey insights discussed below highlight a range of opportunities and challenges for Washington's development, use, and governance of AI technologies. Many of the challenges that people raised during the interviews and survey will be mediated by the release and operation of the policy guidance required by Executive Order (EO) 24-01 Artificial Intelligence. Beyond the tasks called out in the EO, additional actions may be beneficial.

We recommend 7 actions that can be taken by WaTech to further support the responsible use of AI and genAI across the state government.

1. **Review & Monitor**

   Provide a tool to help agencies review and track the effectiveness of their AI technologies, and provide guidance on how to monitor AI technologies.

Rationale	*Implementation & Resources*
69% of survey respondents reported that they lack a systematic process for monitoring the effectiveness of the AI technologies they use.	When selecting new AI technologies to use, especially more complex models, WaTech can investigate the use of built-in monitoring mechanisms. For example, Microsoft offers model monitoring tools within Azure,[6] and Amazon offers model monitoring tools within SageMaker.[7] Many other companies also offer paid model monitoring tools, including WhyLabs, Fiddler AI, Evidently AI, and others.

2. **AI Risk & Impact Assessment**

   Expand existing risk assessment practices, including privacy and security reviews and those developed per the EO for genAI to account for risks and impacts from a full range of AI technologies.

Rationale	*Implementation & Resources*
Survey respondents highlighted the importance of conducting risk and impact assessments for specific AI use cases,	WaTech can provide explicit guidance about how departments should expect to conduct risk and impact assessments for AI

[6] Azure Machine Learning model monitoring, https://learn.microsoft.com/en-us/azure/machine-learning/concept-model-monitoring?view=azureml-api-2
[7] Amazon SageMaker Model Monitor, https://sagemaker.readthedocs.io/en/stable/amazon_sagemaker_model_monitoring.html

especially those that might be high risk to individuals or communities. They also emphasized the need to update privacy and security reviews to better account for novel privacy and security risks associated with AI.	technologies (beyond just genAI), and can formalize and help operationalize updates to the privacy and security reviews. Guidance can similarly draw from NIST's AI Risk Management Framework, the Microsoft Responsible AI Impact Assessment Template,[8] as well as human rights and fundamental rights impact assessments. There are also many resources to draw from for guidance on prevalent AI privacy and security risks, including the OWASP Top 10 for LLM Applications,[9] and the LLM AI Cybersecurity & Governance Checklist.[10]

3. **Acceptable & Unacceptable Uses**

Provide explicit examples of acceptable and unacceptable AI use cases for agencies.

Rationale	*Implementation & Resources*
Many survey respondents expressed interest in having concrete examples of acceptable and unacceptable AI use cases.	Update the interim guidelines to include purposeful and responsible use of genAI, including expanding these guidelines to include a list of acceptable and unacceptable genAI use cases for agencies. Also provide an overarching list of unacceptable AI use cases. For reference, the EU AI Act (Article 5) and the U.S. White House Framework to Advance AI Governance and Risk Management in National Security include prohibited AI practices and use cases.[11]

[8] Microsoft Responsible AI Impact Assessment, June 2022, Templatehttps://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2022/06/Microsoft-RAI-Impact-Assessment-Template.pdf
[9] OWASP Top 10 for LLM Applications, https://owasp.org/www-project-top-10-for-large-language-model-applications/assets/PDF/OWASP-Top-10-for-LLMs-2023-v1_1.pdf
[10] LLM AI Cybersecurity & Governance Checklist, https://owasp.org/www-project-top-10-for-large-language-model-applications/llm-top-10-governance-doc/LLM_AI_Security_and_Governance_Checklist-v1.1.pdf
[11] EU AI Act Annex 3, https://www.euaiact.com/annex/3 and Framework to Advance AI Governance and Risk Management in National Security, https://ai.gov/wp-content/uploads/2024/10/NSM-Framework-to-Advance-AI-Governance-and-Risk-Management-in-National-Security.pdf

4. **Responsible Procurement**

Establish best practices in procuring AI (including under the Direct Buy limit) to inform the development of a verified AI vendors and services list.

Rationale	*Implementation & Resources*
Interviewees and survey respondents highlighted numerous roadblocks to procuring AI tools, as well as uncertainties about how to ensure procured AI technologies would be sufficiently aligned with state laws and guidelines. They also emphasized that guidelines are helpful for small subscriptions that qualify for Direct Buy.	Work with other state procurement officers to share best practices in procuring AI, including contract terms and expectations and Direct Buy guidance to ensure AI uses meet Washington's laws and standards. As an example, in March 2024, the California government published Guidelines on Public Sector AI Procurement.[12]

5. **Transparency & Accountability**

Establish a public-facing AI inventory, as well as clear criteria for when and under what circumstances AI tools should be included in the inventory.

Rationale	*Implementation & Resources*
Interviewees highlighted the importance of transparency for public sector AI use, and survey respondents detailed numerous types of information that should be included in a public-facing AI inventory.	WaTech already published an Automated Decision Systems Inventory in December 2023.[13] This can be updated over time to ensure that it can capture new uses of a variety of AI technologies. Other examples include the Federal AI Use Case Inventory.[14] In March 2024, the Office of Management and Budget issued Guidance For 2024 Agency Artificial Intelligence Reporting Per EO 14110.[15]

[12]State of California GenAI Guidelines for Public Sector Procurement, Uses and Training, https://www.govops.ca.gov/wp-content/uploads/sites/11/2024/03/3.a-GenAI-Guidelines.pdf
[13] Automated Decision Systems Inventory, https://watech.wa.gov/sites/default/files/2023-12/ADS%20Inventory%20Dec%202023%20Final.pdf
[14] Federal AI Use Case Inventory, https://ai.gov/ai-use-cases/
[15] Draft Guidance For 2024 Agency Artificial Intelligence Reporting Per EO 14110, https://www.whitehouse.gov/wp-content/uploads/2024/03/DRAFT-Guidance-for-Agency-Artificial-Intelligence-Reporting-per-EO14110.pdf

6. **Information Sharing**

Facilitate more systematic information sharing across agencies internally, through and beyond the AI Community of Practice.

Rationale	*Implementation & Resources*
Interviewees and survey respondents expressed uncertainty about what other agencies are doing in relation to developing AI policies and exploring AI use cases.	WaTech can help facilitate information sharing across agencies so all interested parties can easily see and share their toolkits, draft policies, training resources, etc. This could be accomplished for example by distributing a monthly announcement, detailing the location of resources, and maintaining internal resource lists.

7. **Mechanisms to Enable Strategic Alignment**

Align opportunities to invest in AI with statewide priorities, agency business objectives, and the needs and priorities of Washingtonians.

Rationale	*Implementation & Resources*
Interviewees and survey respondents emphasized that it will be challenging to accomplish their responsible AI goals without sufficient support, funding, or access to tools, which currently vary across agencies.	WaTech can help to level the playing field across different agencies by providing statewide AI-enabled services, identifying investment opportunities, and ensuring proposed AI investments from agencies align with the State's technology strategy.

Section 2. Washington State Case Study

Overview of Washington's AI Governance Efforts

Washington State is a leader in proactive AI governance. In 2024, Governor Jay Inslee signed Executive Order 24-01 (EO 24-01), establishing a framework for the responsible development, procurement, and use of generative AI systems across state agencies.[16] The order underscores the state's commitment to transparency, accountability, and fairness in AI deployment, ensuring that AI systems enhance government services without harming vulnerable populations. Washington's approach involves continuous engagement with interested parties, emphasizing the need for AI systems to be explainable, non-discriminatory, and auditable. This framework not only provides guidance for AI systems but also offers a roadmap for other states looking to integrate AI into government operations responsibly.

WaTech has also developed interim guidelines for the purposeful and responsible use of genAI.[17] These guidelines serve as an initial framework that enables the state to procure and use genAI responsibly through aligning its actions to the NIST AI Risk Management Framework core responsible AI principles.[18] The guidelines recommend the following actions: (1) fact-checking, bias reduction, and review of AI-generated content; (2) public disclosure and attribution of AI-generated content under certain circumstances;[19] (3) guidance to not use sensitive or confidential data in genAI technologies; (4) compliance of use of genAI with established policies and regulations; and (5) fostering collaboration via the state's AI Community of Practice to share best practices and joint learning. The guidelines conclude with do's and don'ts when using genAI across a variety of applications, such as appropriate use of genAI to aid synthesizing content and communicating to diverse audiences.

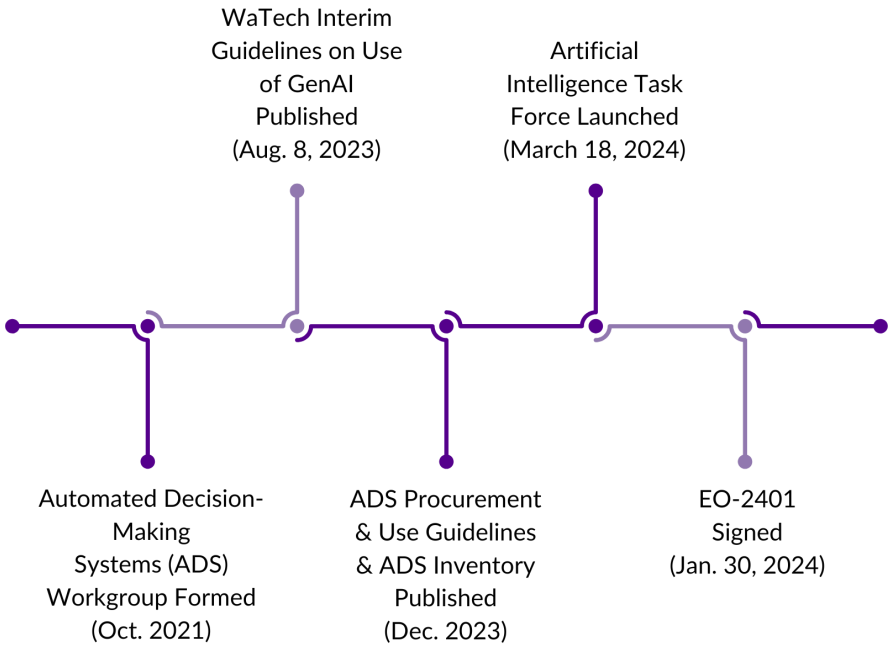
Before EO 24-01, WaTech, in collaboration with a state-wide Automated Decision-Making Systems (ADS) Workgroup, issued its ADS Procurement and Use Guidelines, which serves as a cornerstone of its AI governance framework.[20] Recognizing that AI-driven decisions can have far-reaching consequences, the state established comprehensive guidelines to monitor and evaluate automated decision systems used in public administration. These guidelines aim to ensure that decisions are transparent, accountable, and equitable. As part of this effort, the state has launched initiatives to create tools and processes for auditing these systems, requiring public reporting on ADS use. This focus on transparency and accountability reflects Washington's

[16] State of Washington, 2024, Executive Order 24-01 Artificial Intelligence, https://governor.wa.gov/sites/default/files/exe_order/24-01%20-%20Artificial%20Intelligence%20%28tmp%29.pdf?utm_medium=email&utm_source=govdelivery
[17] WaTech, 2023, Interim Guidelines for Purposeful and Responsible Use of Generative Artificial Intelligence, https://watech.wa.gov/sites/default/files/2023-09/State%2520Agency%2520Generative%2520AI%2520Guidelines%25208-7-23%2520.pdf
[18] NIST AI Risk Management Framework, 2023, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
[19] Guidance on when attribution is necessary is still under development.
[20] WaTech, December 2023, "Automated Decision Systems Procurement and Use Guidance," https://watech.wa.gov/sites/default/files/2024-01/ADS%20Procurement%20Guidance%20-%2012-2023.pdf

commitment to ensuring AI serves the public interest while minimizing risks related to bias, discrimination, or data privacy breaches. In addition to the guidelines, WaTech created a public inventory of ADS applications in use by state agencies.[21]

The state's AI governance efforts are further supported by a commitment to engage with civil society, academia, and industry in developing responsible AI practices. Washington has prioritized an inclusive approach to AI governance, ensuring that practices and policies are informed by diverse perspectives, including those of marginalized groups. This collaborative effort positions Washington at the forefront of responsible AI governance in the public sector, setting an example for other states and national governments.

Timeline of Washington State AI Governance Efforts



Executive Order 24-01 and Generative AI (GenAI)-Specific Efforts

Washington's Executive Order 24-01 establishes a comprehensive framework for managing the use of AI technologies, with particular attention to addressing the unique risks posed by genAI. It recognizes the potential of AI to transform state services and improve efficiency while emphasizing the need to balance these benefits with mitigating risks such as privacy concerns, disinformation, bias, and cybersecurity threats. The order emphasizes the importance of transparency, equity, and ethical deployment, particularly in ensuring that vulnerable and marginalized communities are protected from algorithmic bias and negative impacts of generative AI.

[21] WaTech, 2023, "Automated Decision Systems Inventory," https://watech.wa.gov/sites/default/files/2023-12/ADS%20Inventory%20Dec%202023%20Final.pdf

The order directs various state agencies to collaborate in the development of infrastructure (e.g., sandboxes), guidelines, and risk assessments for the integration of genAI into government operations. Outputs and deliverables from the order are made available on a public webpage.[22] WaTech and the Department of Enterprise Services (DES) are tasked with issuing guidelines for procurement, monitoring, and governance of AI systems, while the Office of Equity will oversee the creation of an accountability framework to ensure fairness and transparency. High-risk genAI systems, particularly those affecting critical areas like healthcare and law enforcement, will be subject to thorough assessment to evaluate their impact on communities and mitigate potential harms.

Additionally, EO 24-01 highlights the importance of workforce training and development in the context of AI. The Office of Financial Management (OFM) will work with WaTech and Washington's Workforce Training and Education Coordinating Board to assess the impacts of genAI on the state workforce and develop programs that equip workers with the necessary skills and knowledge to work effectively with AI. Collaborative research efforts with educational institutions and national organizations are encouraged to foster innovation, expand AI education, and create equitable workforce pathways.

[22] WaTech, 2024, "Reports and Documents," https://watech.wa.gov/about/reports-documents

Timeline of EO 24-01 Deliverables

	LEAD	*DELIVERABLE*
Sept. 2024		
	WaTech	Report of GenAI Initiatives for Agencies
		Initial Guidelines for Procurement
	Office of Equity	Accountability Framework
Dec. 2024		
	WaTech	Guidelines on Impact of Adopting GenAI
		Report on Impact of GenAI on Vulnerable Communities
		Risk Assessments
	Office of Financial Management	Report of Impact of Gen AI on State Workforce
Jan. 2025		
	Department of Enterprise Services	Training Plan for State Workforce
		Contract Terms Template
	Workforce Training & Education Coordinating Board	Identification & Creation of Research Opportunities

The WaTech-Berkeley Collaboration

The WaTech-Berkeley collaboration is an innovative partnership designed to strengthen Washington State's AI governance efforts through research, expertise, and policy guidance. WaTech, the state's technology services agency, has partnered with UC Berkeley to leverage the university's leading research on AI governance, ethics, and public policy. This collaboration focuses on developing guidance on strategies that ensure AI systems used in Washington's public sector are accountable, transparent, and aligned with public values.

The collaboration also fosters knowledge-sharing initiatives, where state personnel receive training on AI governance challenges and best practices. This partnership helps ensure that Washington's integration of AI into its services remains at the forefront of innovation while implementing sound technical and governance practices.

This report is informed by a literature review of current uses of AI in government and emerging responsible AI governance strategies. In addition, in-depth interviews with Washington State personnel and a survey distributed to Washington State and local government representatives provided insights into opportunities and barriers to adopting AI, current uses of AI, and whether agencies have appropriate policies and strategies for responsible AI procurement, development, and use. The following section provides more details on our findings from the interviews and the survey. The Appendices provide further background information about the survey, including the methodology, full list of questions, and figures and graphs to highlight findings from each question.

Interview Findings and Insights

Overview

UC Berkeley and WaTech conducted 12 semi-structured interviews with employees from 10 Washington government agencies throughout the month of March 2024. The agencies included the Department of Fish & Wildlife, the Office of Financial Management, the Department of Natural Resources, WaTech, the Office of Equity, the Department of Health, the Workforce Training and Education Coordinating Board, the Washington State Arts Commission, the Department of Enterprise Services, and the City of Tacoma. The interviewees represented a range of roles, including Director, Manager, and Staff positions, and their varied expertise included technical, legal, and operational areas.

The interviews were held virtually and lasted between 45-60 minutes. The individuals had the option to remain anonymous in write-ups about the findings. The goal of the interviews, as explained to the participants, was to identify opportunities and barriers to development and implementation of artificial intelligence (AI) tools within the Washington state government, including generative AI as outlined in Executive Order 24-01 Artificial Intelligence.

The questions asked throughout the interviews included if and how their organization was using AI or generative AI; their perception of the greatest benefits and risks of using AI and generative AI within their organization; whether there was a process for responsibly developing and/or procuring AI technologies or a process for assessing the potential benefits and risks; whether their organization has principles, policies, or strategies to help guide responsible use of AI or any mechanisms for seeking input from different partners and communities; and how they expected their organization to assess the risk of potentially high-risk or unacceptable risk AI systems. The actual questions explored in each interview were able to dive deeper into particular nuances of these questions depending on the particular role of the individual.

Key Findings

The key findings from the interviews can be grouped into three overarching categories: 1. Disparate patterns of AI use; 2. Responsibility, public trust, and risk aversion; 3. Desire for policy clarity. Each of these categories is discussed further below.

1. **Disparate Patterns of AI Use**

The interviews uncovered that while some agencies have been consciously using AI technologies for many years, other agencies are only more recently beginning to consider using such technologies in the wake of the generative AI boom. The majority of interviewees considered themselves to have relatively low familiarity with and awareness of AI technologies in general, though slightly higher for generative AI, but a couple of agencies (including WaTech) stood out as having much greater awareness. Some of these discrepancies map onto the variance in size and funding of the different agencies.

The kinds of AI uses that people discussed included language translation, image detection (e.g., to identify types of fish underwater, types of animals on land, or smoke in trees), code writing and management assistance, document summarization, transcribing meeting notes, drafting or editing non-sensitive written content, and a knowledge-based internal search engine. People also talked about how AI features have been embedded within other services and tools such as security products for a long time, and that this is only increasing. The vast majority of use cases discussed were only for internal purposes, not resident-facing, and there was a general recognition that public-facing AI use cases involve greater risk. One interviewee discussed a public-facing pilot that visualized policy priorities that had to be shut down because interest was higher than expected and it became too costly to run. This suggests that maintenance costs may be a primary consideration for AI pilots and should be factored into initial assessment decisions.

One theme that emerged was the importance and role of existing enterprise vendor contracts. In particular, because the state has contracts with multiple technology providers that now also offer AI services, it may be more straightforward to assess existing controls and data agreements for those AI services. For example, the state has a Microsoft 365 agreement and many agencies

leverage Microsoft Azure for cloud-enabled services. Microsoft's AI services and tools such as Azure AI and Copilot, can therefore be easier to adopt and integrate into existing workflows. Interviewees discussed the benefits of not needing to go through additional procurement processes to use these tools, but also expressed uncertainty about what they can use based on their existing agreement, and concern about potentially getting locked into sub-optimal offerings or paying for services that may be available for free elsewhere.

Another theme that came up was about personal use versus professional use of AI tools. These findings revealed a continued opportunity in policies and standards on approved resources and tools for the workforce to provide greater clarity on responsible and appropriate use of available tools, as well as on how to align with existing policies and laws on information processing.

Interviewees highlighted a number of barriers to the use of AI technologies including small and overstretched IT teams, data silos, cumbersome procurement processes that can take a year, decision overload and having too many choices, challenges with change management, and funding limitations. One interviewee highlighted that off-the-shelf commercial models do not work for their use cases, and that needing to customize models can add to the expense. Interviewees expressed that some agencies have more funding, personnel, and resources than others and highlighted the need for government-wide adoption of tools and services where possible.

2. **Responsibility, Public Trust, and Risk Aversion**

Numerous interviewees talked about their commitment to responsibility and public trust, and described their agency as risk averse in this context. They recognized the reliance on third parties for providing AI services and tools, and described uncertainty about which vendors and tools could be fully trusted to handle state data and provide real value beyond the hype and marketing claims. Multiple people raised concerns about not wanting to end up in the news for implementing an AI system that goes wrong. People expressed a sense of responsibility and not wanting to contribute to any further erosion of trust in government.

Interviewees raised numerous risks that were top of mind for them with the responsible use of AI. These included privacy threats, reputational risk to agencies (e.g., caused by AI hallucinations or toxic output), supportability of complex technological tools, third-party vendors' data retention policies, liability in the supply chain, not wanting to perpetuate the internet's inequities, and not wanting to use synthetic AI-generated art when they could share real images of Washington life. Some interviewees talked about fear and distrust toward companies producing AI, especially because current legal standards are insufficient to hold companies responsible.

Many people also raised concerns about how AI is affecting and will continue to affect the workforce. All interviewees noted a desire that AI be used to enhance people's work rather than replace it. However, there was a sense that this opportunity will be unevenly distributed and that human labor displacement will be more acute in particular agencies and for particular roles. Some

emphasized the importance of starting with the current reality, which is that they've been trying to do more with less and staff are getting really burned out, and also that the majority of state workers are unionized. The Office of Financial Management has been working with labor partners in assessing the impacts of generative AI on the state's workforce, and is expected to produce a report summarizing their findings in early 2025. Interviewees expressed a desire to use AI to invest back in the workers, and stressed the need to focus on job quality (not just displacement) to understand the ways in which workforce surveillance may increase with the use of AI tools, and to investigate the impact of multiple technological changes simultaneously.

3. **Desire for Policy Clarity**

Interviewees discussed having some existing frameworks and policies to help guide their use of AI. For example, people referenced the framework of sensitivity categories for data (Category 1 data being lowest risk and Category 4 being highest risk) existing privacy and security reviews, and WaTech's interim guidelines for generative AI. At least one interviewee mentioned that there is consideration of adding AI question(s) to the existing secure design submission form and on the privacy threshold analysis. Some agencies mentioned having developed their own additional reports or guidance on AI risks, though in general it seemed that these had not been widely shared with WaTech and other agencies.

However, interviewees generally desired greater clarity about how to think about appropriate uses and different risk levels of AI tools, and felt that they will need additional tools for a full risk assessment beyond the current privacy and security assessments. They mentioned wanting explicit policies they can follow so they know it's OK to move forward and they expressed that reducing uncertainty in this way would help them to embrace the technology with more confidence.

People discussed wanting guidelines about what to ask and ensure from vendors and how to meaningfully assess available tools. Interviewees also expressed a desire to co-create such guidelines with a wide variety of groups including tribal groups and employ techniques such as human-centered design for AI tools to make sure that they, for example, would work for people in rural communities or with visual impairments.

Interviewees expressed considerable interest in gaining access to more training resources as well,on topics including: how to conduct equity assessments in addition to privacy and security assessments, how to recognize AI-produced content, what to tell residents about the authenticity of content, how to recognize instances of bias, how to check for accuracy, how to use the technology in an ethical way, how to use new procurement processes, on what the individual and agency responsibilities are, and on how to communicate about the usage of AI tools externally (for example, when it comes to their use in job applications for government positions). Some agencies have developed their own training resources or have already begun using available training resources, such as on how to use AI for HR work.

Numerous interviewees mentioned looking to WaTech for guidance and leadership on these topics. They also expressed that while it is helpful for agencies to have some autonomy, they would appreciate having consistent guidelines across the state to ensure that some agencies do not have a more lax environment or better access to AI tools than others.

The interview findings suggest that while some agencies and staff are at least moderately experienced and have access to existing frameworks, much more can be done to support the responsible use of AI across Washington state agencies.

Survey Results and Insights

Overview

UC Berkeley and WaTech developed a survey on AI and generative AI, available to anyone in Washington state or local government during the month of May 2024. Respondents were not asked to provide their name or email address. The survey included 19 questions and all of them were optional, so some questions had more responses than others. A total of 131 valid survey responses were submitted, representing 61 different agencies and organizations from across Washington state government, as well as several cities, counties, and local academic institutions.

Please see Appendix C for more information about the methodology and findings from the survey, including additional data visualizations.

Survey Key Findings

The key findings from the surveys can be grouped into seven categories: 1. Widespread AI usage; 2. AI tools are not well tracked; 3. Multifaceted risks and impacts; 4. Varying organizational policies and guidance; 5. Sociotechnical risk and impact assessments; 6. Job automation fears vary by position; 7. Public transparency.

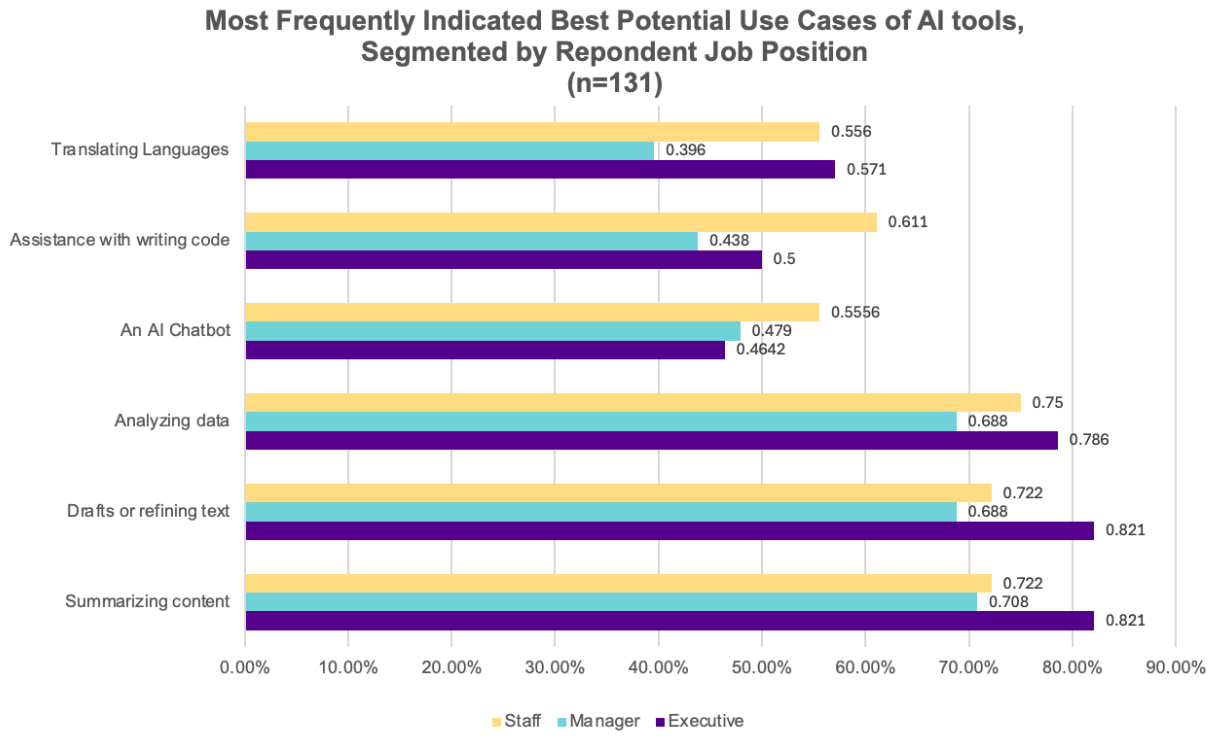
Seven Survey Categories

1. **Widespread AI Usage**

The survey revealed that a significant proportion of Washington state and local government entities have incorporated AI technologies into their workflows. Over half of the respondents (55.7%) reported using AI technologies for official work purposes, while 26.7% do not use AI and 17.6% are unsure if they do. Some agencies, including the Department of Transportation, reported the highest levels of AI implementation in their work.

However, we also found some discrepancies in people's perceptions of organizational use. For example, across financial agencies and social and health agencies a similar number of respondents reported both using AI technologies and not using AI technologies. This suggests uncertainty and misunderstanding within these agencies regarding the extent of AI use. Possible explanations include application of AI tools is limited to specific roles, insufficient inter-departmental communication, or different definitions of what constitutes AI.

The survey results indicated that the highest majority of respondents, more than 76%, were using large language models or generative AI, with smaller percentages reporting using machine learning, predictive analytics, image recognition, or other kinds of AI technologies. The most common AI applications people mentioned included text drafting and summarization, code generation, image recognition, and cybersecurity detection and monitoring. Respondents also found these use cases to be some of the best use cases available for their organization, though they also mentioned others such as analyzing data, translating languages, AI chatbots, and generating images, audio, and video. These answers only varied to a small extent, depending on the role (e.g., manager, executive, or staff).



2. AI Tool Tracking

Despite the relatively high uses of AI tools, most respondents reported that they did not monitor or track their effectiveness. Sixty-nine percent of respondents reported that they lack a systematic process for monitoring the effectiveness of the AI technologies they use. Only a small percentage of the organizations surveyed conduct periodic reviews of AI systems, with 5.6% conducting annual reviews and 4.2% conducting quarterly reviews. While the state has implemented strategies to track AI projects, there is a lack of consensus on *how* these AI technologies should be tracked. Some agencies are thinking through strategies for evaluating return on investment (e.g., to productivity gains) in relation to impact assessments that evaluate risk of harm (e.g., to equity).

3. Multifaceted Risks and Impacts

Survey respondents were asked about what they think are the biggest risks, challenges, and concerns associated with using AI within their organizations, and many people selected multiple answers. Privacy risks (76.0%) and accuracy and reliability (76.0%) were the most frequently identified potential risks of AI use. However, the potential for misuse, labor rights concerns, equity concerns, copyright and fair use concerns, and security risks were also commonly selected. Environmental impact was relatively less important in people's minds (selected by only 18.6% of

respondents). People also mentioned concerns with data storage and data sources, AI hallucinations, and lack of education.

Respondents from different types of roles largely shared similar concerns, though for some risks opinions diverged. For example, our analysis showed that security risks related to AI vulnerabilities are top-of-mind for many managers (72.9%) and executives (71.2%). However, this concern was significantly less prominent among general staff, with only 44.4% of staff respondents identifying it as a potential risk. This disparity may indicate a lack of awareness among employees regarding how AI systems can carry security vulnerabilities, with organization leadership being more cognizant of these risks. The significantly lower level of concern among employees might suggest a need for education and training to build their understanding of AI-related security threats.

4. Varying Organizational Policies and Guidance

The survey results show that 39.6% of organizations have established AI policies or implemented interim AI guidance (including WaTech guidelines), while 37.7% have no policies in place. Additionally, 13.2% are developing policies, which involves convening task forces or workgroups to discuss policy options and write policy drafts. A small percentage of respondents are either unsure (6.6%) or have proposed new policies that are currently under review (2.83%). These results indicate that many organizations have been proactive about incorporating AI governance into their department workflows, but levels of sophistication vary, ranging from high-level descriptions of what to avoid to more detailed guidance.

Respondents expressed a need to ensure clarity and information-sharing about what already exists, for example at the Washington Department of Ecology and the Washington Traffic Safety Commission, as well as what is being developed by the Washington State Department of Labor and Industries and the Washington State Department of Transportation, and to review the Washington State Health Care Authority's AI Ethics Framework.

Many respondents hope to have additional support for the responsible procurement of AI technologies within their organization. In particular, respondents were eager to have examples of acceptable and unacceptable use cases, an AI tool assessment process, and a new AI vendor assessment process and approved AI vendor list. Additional guidance that people highlighted included having statewide principles, policies, and guidelines; having a regulatory compliance assessment process; security controls for AI; and contract language specifications including consequences for failure and termination conditions as well as restrictions on agency data use.

A majority of respondents also emphasized the need for amendments to established privacy and security reviews to ensure appropriate identification and mitigation of risks. In order to achieve this, respondents emphasized the importance of state-level policies to standardize approaches across the state. This would include not only creating new policies but also amending established policies (e.g., those that led to the development of existing privacy and security reviews) to ensure alignment with best practices from industry, academia, and government. The policies should be agile, allowing for modification as the technology quickly evolves. Respondents noted the potential to use the NIST AI Risk Management Framework to evaluate AI risks and support the broader mission of standardizing approaches across the state.

5. Sociotechnical Risks and Impact Assessments

Respondents also identified key considerations they would like to see included in an AI risk assessment. For example, they noted that any risk assessment process should include bias and equity reviews and should be tailored to specific AI use cases, especially those that pose a high risk to individuals or communities. Respondents also thought it would be important to address intellectual property of AI-generated content, including how to communicate this to the public.

Respondents recommended integrating AI risk assessments into existing workflows to streamline processes and include AI-specific thresholds and questions based on risk, use case, and complexity. They emphasized focusing on the "people side" of risk assessments, considering the impact of AI-generated results on organizational reputation and trust, mental health, social interactions, and jobs. Comprehensive risk identification should cover security, privacy, fairness, accountability, bias, and algorithmic impact. Guidelines for government-used generative AI should address privacy, equity/non-discrimination, attribution/intellectual property, ensuring compliance with ethical, security, and privacy standards. Several respondents noted the importance of using the NIST AI Risk Management Framework to inform any risk assessment processes.

Privacy

Respondents are concerned about appropriate data management and security, calling for clarity on data access, sharing permissions, and mechanisms to keep data private, especially when dealing with a third-party vendor. In order to achieve this, respondents recommended training data owners and partners on responsible data management and AI use. The state should maintain plain language guidelines with examples of the application of genAI across various use cases. These guidelines and examples can help guide evaluation of vendors and continuous monitoring of procured products and services, especially as their application areas may change over time.

Equity/Non-Discrimination

Respondents were also asked to consider what should be included in an AI impact, equity, and bias assessment. Survey respondents noted the need to conduct assessments of data privacy, security, quality, and representativeness; bias and fairness; vulnerability to attacks; intellectual property theft; social, economic, and environmental impacts; and compliance with applicable laws and policies within a specific domain area. One respondent noted the need to continuously monitor generative AI, including the data it is trained on and learning from, to mitigate its creation of harmful outputs. One respondent noted the importance of evaluating effects on mental health and well-being from the use of genAI by state personnel as well as these effects within the communities served. Several noted the need to integrate community and employee feedback, especially those of diverse backgrounds, to guide appropriate risk and impact assessments and mitigations.

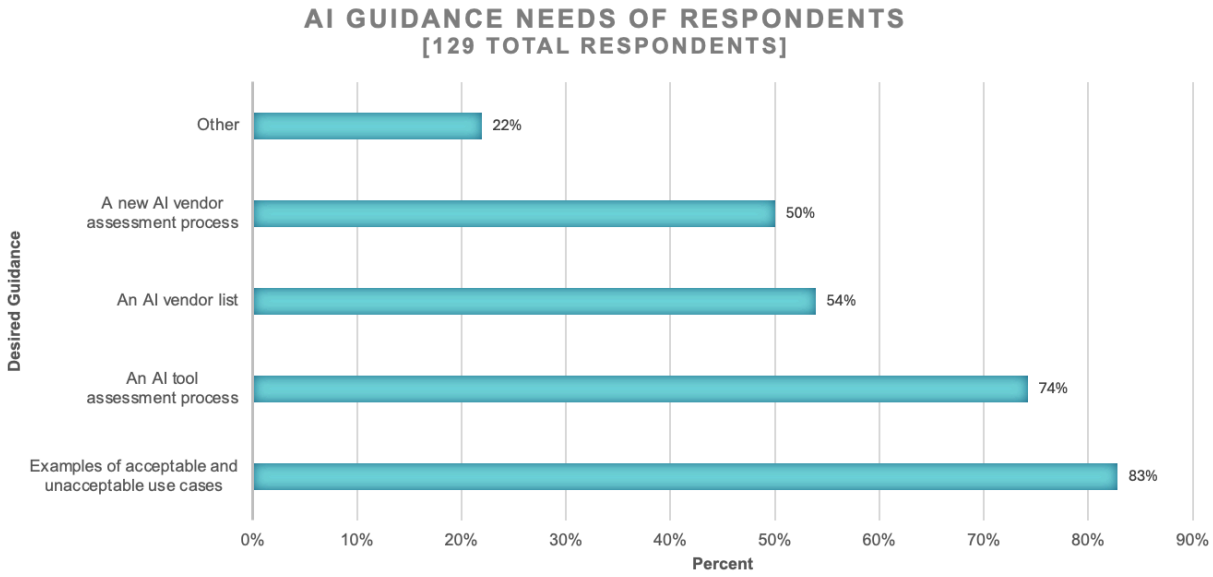
Attribution/Intellectual Property
Respondents were also asked about what features or contexts of use should contribute to an AI system being classified as high risk or unacceptable risk. Many of the possible choices were popular, including if the system introduces significant security risks, is prone to error or hallucination, uses sensitive data, is used in a high risk domain, is prone to malicious use, or works less well for certain groups. People also named some additional considerations including if the system is not explainable or if the design of the application is such that it would lead to attachment or facilitate relationships with people, especially emotionally vulnerable populations.

6. Job Automation Fears Vary by Position

Nearly two-thirds (64.5%) of respondents said they think AI is "likely to significantly improve efficiency and effectiveness of the state workforce." And a majority also thought that AI was likely to augment tasks that people carry out and would change the way most people in the state workforce carry out their work. However, 37.9% thought that AI is likely to fully automate some current jobs. And some respondents emphasized the risks, noting that AI is likely to reduce the quality of work produced and lead to less retained organizational and technical knowledge. It is noteworthy that some respondents had opposite impressions about the impact of AI, for example some thought it would reduce the quality of work and overwhelm workers, while others thought it would increase efficiency and ease workers' burdens. We found that general staff (42.9%) are the most concerned about job automation, whereas executives (33%) and managers (26.7%) consider it to be less of a possible impact on the state workforce. These results indicate a difference in perception, with frontline employees feeling more at risk of job displacement due to automation compared to their higher-ranking counterparts.

Survey respondents were generally interested in having training resources. Many respondents indicated a desire for comprehensive on-going training that touches on all aspects of responsible AI practices, including: privacy, security, safety, ethics, and methods for validation. Respondents also emphasized the need to include diverse internal and external interested parties in the development, implementation, and completion of this training. 68.5% of respondents thought that having "responsible AI champions" within their organization could help with these efforts, though 28.3% were unsure, perhaps because they were not sure exactly what this would entail.

Respondents flagged other kinds of guidance and support as important including technical guides and tips, clarity about what counts as AI, accountability from WaTech on all AI use by state technology domains, approved vendors, annual audit processes, code review processes, AI evaluation tools, how to disclose the use of AI at work, and how to document AI tools. People also mentioned wanting to coordinate across state privacy and security staff, to include social scientists and not just "AI professionals," to hire additional staff tasked with this responsibility, and funding to effectively manage AI. Many respondents mentioned wanting to hear about real-world, practical use cases and to learn from the experiences of people in their community. Many respondents also desired clear policies and guidelines to follow.



7. Public Transparency

Survey respondents were asked what information should be included in an inventory, including what information should be made public. The following table provides a summary of their responses.

Many respondents argued that all uses of AI by the state government should be made transparent and made comments along the following lines: “I think all should be made public for transparency reasons,” or, “I think we should make as much as possible public.” One respondent added the qualifier, “where privacy/security would not be compromised, I think transparency is an absolute must to gain public trust.” One respondent notes, “Please refer to the transparency ethical consideration in the HCA AI Ethics Framework.” Several respondents pointed out that the duty to inform the public is especially high if it is a public-facing tool.

Some respondents raised concerns about having an inventory. One respondent felt that a state inventory is not particularly useful and worried that people should not have to report every time they use Microsoft Copilot. Another noted that if AI is embedded in most state work soon, it will be excessive to document each use and instead the inventory should be used for “high-profile” uses. Some respondents suggested that each unique use case should be included, while others suggested that the inventory would be used to document types of use cases, an approved tools list and approved use cases. Multiple respondents felt that a public-facing inventory was a critical element of maintaining public trust. People also noted that an inventory will help internally to reduce redundancy and see what tools other agencies are using.

Respondents' Views on What Should be Included in an AI Inventory

Purpose

- Expected benefit
- Why is AI needed (i.e., what problem is it solving)?

Data Management

- Type & category of data used, whether it includes state data
- Training data & information sources used
- Data sharing agreements, restrictions, & obligations

Technology, Tools, & Vendors

- Software used that includes description of functionality, including underlying model/architecture
- Cost
- The vendor(s), if applicable, and tool(s) used by Washington
- Internal developers, if applicable, and tool(s) used by Washington
- Integration and connectivity with existing systems (e.g., software & hardware; network devices & endpoints)

Users & Partners

- Who is using the tool (agency, team, number & type of users, e.g. for individual or industrial use)
- Target audience (e.g., only internal or external)
- Training guides

Risk & Impact Assessment

- Risk assessment and risk category/level
- Risk mitigation strategies
- Ethical concerns
- If evaluation/ verification/validation methods are used, and the most recent date of verification
- Ratings of accuracy of AI performance, including errors made
- Impact to workforce (estimation of replacement/augmentation of human labor)
- Environmental impact
- Expected and actual impacts

Monitoring & Oversight

- A contact person for each use case
- Oversight approach
- Controls used to mitigate the impact of inaccurate AI-derived information products
- Privacy and security controls in place to safeguard the data
- Compliance/audit functions

Section 3. Existing and Potential Applications of AI Within the Public Sector

The Use of AI within the Public Sector: Introduction

Federal, state, and local government agencies across the United States are increasingly deploying AI-enabled tools to improve public service delivery. These tools range from resident-facing services designed to provide direct assistance for accessing public services, to internal tools that help government employees streamline their daily operations and more effectively carry out their core functions. In this section, we explore these applications by providing examples and analysis into the obstacles encountered during beta testing and release.

This section provides an overview of the history of AI's use in the public sector and identifies three types of AI technologies and tools currently in use by the public sector: (1) Chatbots for resident Services, (2) Generative AI (genAI) for Content Creation, and (3) Machine Learning and Predictive Analytics. The goal in this section is to describe the current state of application by government agencies and to derive lessons learned and best practices from case studies to understand what constitutes a successful deployment of an AI-enabled tool in government work. Our aim is for this information to help readers identify pitfalls during the launch and implementation phases, and to highlight the benefits and drawbacks of the use of such tools. Additionally, this section looks ahead to emerging trends and the future of AI deployments in government.

Overview of AI in the Public Sector: A Brief History

The adoption of artificial intelligence (AI) in the public sector has evolved rapidly since its initial use in the mid-2000s. Governments around the world first explored AI for enhancing data management, improving decision-making, and automating routine tasks. Early implementations included fraud detection, traffic management, and predictive policing. By the late 2010s, AI-driven systems had expanded into healthcare, education, and social services, as machine learning models gained the ability to analyze large datasets and identify patterns. Today, AI continues to transform the public sector, with governments increasingly leveraging AI for everything from resident engagement to infrastructure management.

Recently, generative AI (genAI) has sparked renewed interest in exploring AI's role within the public sector. Governments have started recognizing the potential of genAI to provide enhanced community services via interactive chatbots, synthesizing and communicating information to diverse audiences, and streamlining internal paperwork processing.

Types of AI Technologies and Tools in the Public Sector

1. Chatbots for Resident Services

AI-powered chatbots have become increasingly visible on government websites at the state, local, and federal levels for the purpose of streamlining communication between governments and residents. Many municipalities and federal agencies now employ chatbots to handle routine inquiries such as filing taxes, scheduling services, or reporting local issues. These tools make government interactions more efficient and accessible by automating responses to frequently asked questions about public services, guiding users through government processes, and providing 24/7 assistance to residents. Agencies hope that these chatbots reduce the workloads of government employees, enabling them to focus on more complex, skill-intensive tasks. While the sophistication of these chatbots varies significantly, AI remains a key component in each.

The simplest and most commonly used chatbot by government agencies are **rule-based chatbots**. Utilizing a simpler subfield of AI known as natural language processing (NLP), these traditional chatbots facilitate prompt-based interactions by guiding users through scripted back-and-forth "conversations" that follow predefined rules. User queries are matched to specific keywords, which trigger predefined responses intended to answer frequently asked questions. These chatbots work well for handling common inquiries in a quick, consistent, and reliable way. However, these chatbots are often limited to specific subjects and struggle with questions on topics outside of the training data or those phrased in unique ways. Their ability to understand context and learn from user interactions is also severely limited.

LLM-powered chatbots are a major advancement over rule-based systems, using deep learning models trained on massive amounts of textual data to understand and produce human language. Unlike rule-based chatbots, LLMs can understand user intent and context and therefore handle unexpected queries more effectively. For government use, these chatbots typically start as foundational LLMs pre-trained on general purpose datasets which are then fine-tuned with agency-specific data. This customization process improves the chatbot's ability to provide accurate, relevant responses based on the specialized information and workflows required by the agency. However, LLM chatbots frequently misinterpret input or make mistakes that require performance oversight.

> **MyCity NYT Chatbot**
> In October 2023, the City of New York launched an LLM chatbot to provide local small business owners access to information and answers to questions about starting and operating a business in New York City (NYC).[23] Developed by Microsoft and trained on information from over 2,000 NYC Business web pages, the MyCity NYT Chatbot was designed to help small business owners navigate compliance with city codes and regulations and more easily access business resources offered by the city. Before accessing the chatbot, users must agree to its beta limitations via a disclaimer message explaining

[23] Governing (Oct. 2023), New York City Launches Government Info Chatbot, https://www.governing.com/infrastructure/new-york-city-launches-government-info-chatbot

that the chatbot is still in a piloting period and may provide incomplete or inaccurate information. Users are advised to validate all information provided by the chatbot with the official information hosted on NYC's city website. A red-teaming investigation exposed the fallibility of the chatbot, revealing several instances of the chatbot providing incorrect and misleading information that contradicted City policies and recommending explicitly illegal practices to small businesses.[24] For example, the chatbot gave erroneous advice regarding landlord-tenant and consumer and labor protection regulations. The chatbot also lacked consistency, often providing different responses to the same prompt, making it difficult to reproduce or predict errors. Despite these issues, the City decided to keep the chatbot operating while working with Microsoft to improve its performance and accuracy.

Takeaway
NYC implemented an adaptive strategy to deploy an experimental AI tool in local government to automate some of its public services. The city accomplished this by protecting itself from liability through a tool disclaimer, addressing negative press directly, and continuing to develop and refine the tool. This approach allowed NYC to keep the chatbot available for small business owners, not throw away their investment, while iteratively improving its performance.

2. GenAI for Content Creation

Governments are also exploring the use of generative AI to aid in drafting documents, writing speeches, and other administrative tasks. For example, GenAI models can generate first drafts of policy documents, reducing the time civil servants spend on routine writing tasks. Several states are looking to implement genAI to automate the preparation of legal documents and other administrative paperwork, such as Medicaid fulfillment.[25] The deployment of these tools within government workstreams is still in its early stages, and these tools currently have significant limitations that require a 'human in the loop' to provide oversight over their outputs and ensure their accuracy.

Department of Defense's AcqBot

In 2023, the U.S. Department of Defense (DoD) began prototyping AcqBot, a generative AI-powered tool designed to expedite the procurement process by automating the initial drafting of federal government contracts.[26] Developed by the Pentagon's Chief Digital and

[24] Offenhartz, J. (April 3, 2024), NYC's AI chatbot was caught telling businesses to break the law. The city isn't taking it down, *AP*, https://apnews.com/article/new-york-city-chatbot-misinformation-6ebc71db5b770b9969c906a7ee4fae21
[25] Cho, T. & Miller, B. (Feb. 2024), *2*(2), Using Artificial Intelligence to Improve Administrative Processes in Medicaid, *Health Affairs Scholar*, https://academic.oup.com/healthaffairsscholar/article/2/2/qxae008/7591560
[26] Heckman, J. (Feb. 9, 2023), DoD builds AI tool to speed up 'antiquated process' for contract writing, *Federal News Network*, https://federalnewsnetwork.com/contracting/2023/02/dod-builds-ai-tool-to-speed-up-antiquated-process-for-contract-writing/

AI Office (CDAO) and its Tradewind Initiative, AcqBot uses text-generation LLMs to draft user requirements, industry outreach materials, solicitations, and agreements.[27] Government technology procurement is a time-consuming, bureaucratic process that involves the drafting of solicitation details, regulation citations, and contract agreements. AcqBot is being tested and fine tuned by DOD to assist with these tasks. Trained on a dataset of government contracts, AcqBot is dependent upon human oversight throughout the draft generation process to ensure accuracy. The Pentagon aims to continue refining the performance of AcqBot to a point where it can reliably automate the initial drafting of contracts, producing boilerplate templates for contracts and shortening the timeline for government workers to acquire defense technology for service members.

Takeaway

Government procurement is a notoriously slow and cumbersome process. AcqBot represents an effort by bureaucrats to help remove some of the procedural bottlenecks by introducing a subject-specific genAI tool. Limited public information is available about the tool and its rollout. However, a key feature of the tool advertised on the vendor's website is its ability to routinely prompt users for human review throughout the contract generation process. This feature serves a dual purpose: it appeals to government agencies that require human oversight as a safeguard and acts as a quality assurance measure to mitigate the risks of model hallucinations and errors.

3. Machine Learning and Predictive Analytics

New applications of ML technology and predictive analytics are revolutionizing how governments extract value from their data. Agencies are using these tools to improve operational efficiency and optimize resource management in areas like waste management, traffic management, law enforcement, social service allocation, and emergency response. By contracting with the private sector, agencies are able to introduce new tools that help facilitate informed government decision-making in automated and scalable ways to operate more cost-effectively and sustainably – ultimately improving the ability of agencies to respond to the needs of residents. However, these tools also carry significant risks, as their decisions can have profound impacts on residents' well-being. In healthcare, predictive models have been used to allocate resources during public health crises, such as in the COVID-19 pandemic. In the U.K., ML algorithms helped identify high-risk populations to ensure timely vaccination distribution.[28] In the U.S., predictive analytics

[27] https://www.tradewindai.com/ai-acquisition-playground

[28] United Kingdom Central Digital and Data Office, (June 1, 2022), "Department for Health and Social Care and NHS Digital: QCovid Algorithm," https://www.gov.uk/government/publications/department-for-health-and-social-care-and-nhs-digital-qcovid-algorithm

have been used to improve transportation planning, such as predicting traffic patterns and optimizing infrastructure investments in cities like Boston and Seattle.[29]

Washington Department of Natural Resources (DNR) Pano AI Wildfire Detection

Due to climate change, Washington State now experiences more devastating wildfire seasons that last for longer and fires that burn at a higher acreage rate.[30] [31] The agency has shifted its response strategy to prioritize stronger initial responses to wildfires when they are more manageable, aiming to contain 95% of fires to fewer than 10 acres.[32] To accomplish this, the Washington Department of Natural Resources (DNR) has embraced using AI technology to detect and extinguish wildfires more quickly and effectively.[33] Washington DNR has partnered with the disaster preparedness technology start-up Pano AI to install ML-powered cameras at wildfire lookout points in high-risk fire areas across the state.[34] This tool enables DNR to detect fires sooner, dispatch firefighters faster to control the burn, and conserve vital state resources – thereby reducing costs and saving lives and property. Pano AI's computer vision systems are capable of detecting smoke plumes in forests, distinguishing the type of smoke, and alerting DNR dispatchers to fires.[35] Utilizing satellite data, Pano AI cameras can also determine and transmit the location coordinates of a fire's epicenter or bearing line to direct first responders. Once a fire is burning, Pano AI's 360-degree cameras provide optical zoom feeds for fire dispatch centers to assess and monitor fire behavior. This combination of visual and geolocation data helps guide the DNR's response and track the progression of a fire. Since beginning the pilot in March 2023, 21 cameras have been installed in Washington.

Takeaway

DNR's partnership with Pano AI showcases how AI technology can be effectively implemented by government agencies to address environmental challenges exacerbated by climate change more efficiently and in a cost-effective way.

Google Research's Green Light Initiative

In 2022, Seattle became the first city in North America to partner with Google Research's Green Light initiative, a project utilizing Google's AI tools and Google Maps driving trend

---

[29] Andrews, J. (Aug. 15, 2024), "Boston Uses AI to Reduce Stop-Go Traffic by 50 Percent," CitiesToday, https://cities-today.com/boston-uses-ai-to-reduce-stop-go-traffic-by-50-percent/

[30] Swanson, C. (Aug. 19, 2023). "WA's wildfire seasons will last longer, cut deeper," https://www.seattletimes.com/seattle-news/was-wildfire-seasons-will-last-longer-cut-deeper/

[31] Dennis, E. (Aug. 28, 2023), "Wildfire seasons in Washington are lasting longer and burning differently," The Spokesman Review, https://www.spokesman.com/stories/2023/aug/28/in-wa-wildfire-seasons-are-lasting-longer-and-burn/

[32] Chronicle Staff, (April 18, 2024), In focus: Washington DNR prepares for wildfire season with mock fire exercises in Capitol Forest, *The Chronicle*, https://www.chronline.com/stories/in-focus-washington-dnr-prepares-for-wildfire-season-with-mock-fire-exercises-in-capitol-forest,338695

[33] https://www.pano.ai/

[34] https://www.pano.ai/

[35] https://www.dnr.wa.gov/news/commissioner-franz-pano-ai-and-t-mobile-provide-update-how-ai-tech-and-5g-are-helping-dnr-fight

data to manage traffic signal timing at city intersections.[36] Piloted at 70 intersections in 14 cities across three continents thus far, Project Green Light aims to improve traffic flow and reduce vehicle emissions, with Google Research estimating reductions of up to 30% in traffic stops and up to 10% in CO2 emissions in cities where it is implemented.[37] Google approached the Seattle Department of Transportation (SDOT) because of its advanced traffic engineering department and experience integrating new technology. Historically, SDOT has designed traffic signal timing plans using community feedback, field observations conducted manually or by sensors, and traffic prediction software. Now, Google's Green Light models traffic patterns for several intersections in Seattle and builds timing adjustment recommendations for SDOT engineers, who consider them alongside their own findings drawn from traditional data sources and decide whether to implement changes.

Takeaway
This collaboration augments rather than replaces SDOT's existing signal timing engineering process. Moreover, Green Light provides quick feedback on the effectiveness of any accepted signal timing changes, enabling SDOT to revert if found ineffective. This project, which has expanded to more intersections over the years, represents an innovative public-private collaboration between city government and Big Tech to integrate AI technology into public services for the purpose of optimizing efficiency and improving environmental sustainability. One unique aspect of this particular case is how an AI application for traffic management can also support cities' sustainability goals by reducing emissions and unnecessary energy use.

Section 4. Opportunities & Barriers to AI Adoption

The public sector faces unique opportunities and barriers to AI adoption. In some cases, governments face personnel and resource constraints and stand to benefit significantly from potential efficiency gains from AI technologies. However, these same constraints can make it harder to thoroughly assess potential new tools or to engage in rigorous monitoring of tools put in place.

Within the public sector, AI technologies are generally being applied to a range of functions including efficiency of internal operations, internal and external oversight for greater accountability, responsiveness of public services, and effectiveness of policymaking. In particular, improving efficiency through the automation of simple, repetitive tasks is a primary use case for the public sector. For example, the US Patent and Trademark Office uses AI tools to support the processing of patent applications by helping identify relevant documents and areas of existing

[36] American Planning Association, 2024, Green Means Go: Seattle's AI Solution to Reduce Stoplight Idling, https://www.planning.org/planning/2024/mar/green-means-go-seattles-ai-solution-to-reduce-stoplight-idling/
[37] Google Research, 2024, Greenlight, https://sites.research.google/greenlight/#intro

knowledge.[38] Many other examples of public sector use of AI are described in the previous section. Despite these opportunities, there are technical, ethical, and legal constraints to using AI in the public sector, which we discuss below.

The technical constraints of AI technologies vary significantly depending on the type of AI in use. For relatively simple models, for example supporting robotic process automation (RPA), the outputs of a model may be consistent and reliable - for each given input, there will be a particular output. However, large language models and generative AI are significantly more complex and are non-deterministic - they can produce different outputs for the same input. Their complexity makes them more capable of advanced understanding tasks, but this benefit can come at the cost of reliability. Moreover, it is much harder to understand the full internal working of advanced AI systems. These systems learn for themselves based on (in some cases unimaginably large) training datasets rather than from top-down design, and it can be impossible to know exactly what they have learned. For example, the most advanced large language models have hundreds of billions of parameters (the numerical values that encode the knowledge and skills of a model and determine how a model turns inputs into outputs). Current methods to improve the transparency and explainability of advanced models are unreliable and tend to be oversimplified.[39]

In addition to these challenges with reliability and interpretability, other technical, ethical, and legal constraints associated with AI technologies include the difficulty in fully preventing undesirable behaviors in models. For example, large language models can leak private, sensitive, or copyrighted information;[40] they exhibit gender, racial, social, and political biases;[41] they can be extremely computationally, energy, and resource intensive to train and run leading to significant environmental costs;[42] and they have persistent security vulnerabilities including susceptibility to 'jailbreaking' or getting around safeguards and constraints.[43]

Another primary consideration for the use of AI in the public sector is the impact on the workforce. One study found that around 40 percent of tasks performed by public-sector workers could be done by AI, but that a much smaller number could be fully replaced by AI.[44] As discussed in the Washington State Case Study, many government employees have concerns about how AI may change and automate jobs in the near future.

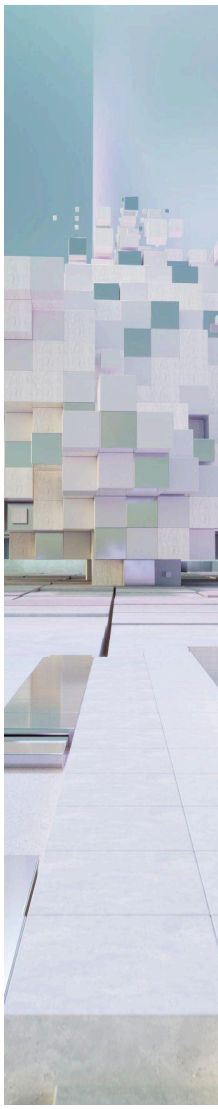
---

[38] G7 Toolkit for Artificial Intelligence in the Public Sector, https://www.oecd.org/en/publications/g7-toolkit-for-artificial-intelligence-in-the-public-sector_421c1244-en.html
[39] Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability, https://journals.sagepub.com/doi/10.1177/1461444816676645; Grokking Group Multiplication with Cosets, https://arxiv.org/abs/2312.06581
[40] Copyright violations and large language models, https://aclanthology.org/2023.emnlp-main.458
[41] Dialect prejudice predicts AI decisions about people's character, employability, and criminality, https://arxiv.org/abs/2403.00742
[42] The Price of Prompting: Profiling Energy Use in Large Language Models Inference, https://arxiv.org/html/2407.16893v1
[43] Jailbreaking ChatGPT via Prompt Engineering: An Empirical Study, https://arxiv.org/abs/2305.13860
[44] The Potential Impact of AI on the PublicSector Workforce, https://assets.ctfassets.net/75ila1cntaeh/5lQnxbf9GVYWmqdPuDgfla/72253fa2e00ee15b0887d2690891e42d/Tony_Blair_Institute_for_Global_Change__The_Potential_Impact_of_AI_on_the_Public-Sector_Workforce__July_2024.pdf

As governments seek to reap the benefits and overcome the barriers to AI adoption, it is particularly important to assess the appropriateness of particular AI use cases. This entails rigorous risk assessments and impact assessments, as well as engagement with community partners and affected communities, during the design or procurement phases to make sure that the type of AI technology and the tool or service proposed is best suited to the problem at hand. These processes are discussed in more depth in Section 6 on the Strategic Roadmap.

Section 5. Responsible AI Governance Strategies & Best Practices

Responsible AI governance has emerged as a foundational requirement for ensuring that AI-enabled technologies are deployed in ways that align with ethical standards and mitigate potential harms. This section explores the principles, strategies, and policy recommendations crucial for promoting responsible AI, referencing foundational literature that provides a framework for understanding these concepts.



Understanding Responsible AI: Key Principles

Responsible AI encompasses a set of values-based principles that emphasize the importance of transparency and explainability; inclusivity and fairness; accountability; robustness, security, and safety; privacy; and sustainability in AI development and deployment.[45] These principles are central to ensuring that AI not only serves the public good but also respects individual rights and social values.

Managing Risks: Strategies for Addressing Constraints and Risks

To address the risks and constraints associated with AI, effective governance strategies must include continuous training, regular ethical AI audits, and active partner engagement. Continuous training allows both AI developers and end-users to remain informed about the evolving nature of AI risks and ensures that they are equipped to handle the nuances of AI-driven decisions. Ethical AI audits are essential for identifying and mitigating potential biases, fairness issues, and privacy concerns before they become embedded in AI systems.[46] These audits provide a structured process for examining AI's impacts, offering transparency to interested parties and promoting trust in AI deployments. Interested party engagement is equally critical, involving a broad coalition of voices, including policymakers, industry experts, and civil society. Surveys and interviews conducted in studies such as the UN's B-Tech report underscore that involving affected communities and interest groups can lead to AI systems better aligned with societal expectations and ethical norms, as well as improved adoption and understanding of AI solutions in diverse sectors.

[45] OECD AI Principles Overview, https://oecd.ai/en/ai-principles
[46] Google Deepmind, Evaluating Social and Ethical Risks from Generative AI, https://deepmind.google/discover/blog/evaluating-social-and-ethical-risks-from-generative-ai/

Values-Based Responsible AI Principles

Transparency & Explainability - Decision-making processes and data sources driving AI outcomes should be clearly communicated.[47]

Inclusivity & Fairness - Biases within AI systems should be managed to prevent discrimination and unequal treatment across different demographic groups[48]

Accountability - Entities deploying AI must be answerable for their systems' actions and impacts.[49]

Robustness - AI models perform reliably under a range of conditions, reducing risks of unexpected outcomes.
Security - Protect systems from cyber threats and unauthorized access.
Safety - Test and monitor to prevent harmful impacts.[50]

Privacy - Personal information must remain secure and processed in ways that respect individual autonomy. [51]

Public Purpose & Social Benefit - Use of AI should deliver better and more equitable services and outcomes to beneficiaries.

Sustainability - AI projects should consider environmental and societal impacts and utilize energy-efficient designs and long-term viability.[52]

---

[47] US White House, Office of Science and Technology Policy, Blueprint for an AI Bill of Rights, https://www.whitehouse.gov/ostp/ai-bill-of-rights/; NIST Artificial Intelligence Risk Management Framework, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

[48] NTIA AI Accountability Policy Report, https://www.ntia.gov/issues/artificial-intelligence/ai-accountability-policy-report

[49] OMB Memorandum on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence, https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf

[50] US Cybersecurity and Infrastructure Security Agency (CISA), Guidelines for secure AI system development, https://media.defense.gov/2023/Nov/27/2003346994/-1/-1/0/GUIDELINES-FOR-SECURE-AI-SYSTEM-DEVELOPMENT.PDF; GAO, Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities, https://www.gao.gov/assets/gao-21-519sp.pdf

[51] US White House, Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, *https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/*

[52] NTIA AI Accountability Policy Report, https://www.ntia.gov/issues/artificial-intelligence/ai-accountability-policy-report; United Nations B-Tech, Taxonomy of Human Rights Risks Connected to Generative AI, https://www.ohchr.org/sites/default/files/documents/issues/business/b-tech/taxonomy-GenAI-Human-Rights-Harms.pdf

Aligning AI Governance with Values

To further align AI governance with values, it is important to implement strong data privacy protections, establish bias detection and mitigation protocols, and set stringent standards within procurement policies to ensure that only vetted AI systems are acquired for public sector use.[53] Integrating these elements into existing policies, such as data protection and privacy policies, supports a comprehensive and layered approach to AI oversight. Additional strategies, such as requiring licenses for AI software, establish accountability mechanisms and promote responsible innovation. Finally, integrating oversight into existing policy frameworks, such as through periodic reviews and regulatory updates, strengthens the ethical and operational guardrails for AI systems.[54] Together, these practices and policies create a robust infrastructure for responsible AI governance, leveraging existing regulatory frameworks and advancing procurement standards to ensure AI systems align with societal values and ethical norms.

Section 6. Strategies to Enable Responsible Public Sector AI Governance & Use

In promoting responsible AI in the public sector, various federal and state strategies are shaping the governance landscape for responsible AI development and use.

Federal AI Governance Strategies

The United States federal AI governance strategy is designed to promote responsible AI development, deployment, and oversight. It aims to balance innovation and national security with ethical standards and public trust, ensuring that AI systems are used safely and effectively across federal agencies and in public-private partnerships. The strategy includes the use of legislation, executive orders and agency guidance, and voluntary commitments.

Legislative Framework

Several legislative initiatives in Congress address AI's diverse challenges and opportunities. These bills cover areas such as mitigating bias and discrimination in AI, fostering transparency and accountability, and enhancing workforce retraining to prepare for the technological shifts AI brings. Among the few enacted into law, two prominent examples are the National AI Initiative Act and the National AI Training Act.

---

[53] US Cybersecurity and Infrastructure Security Agency (CISA), Guidelines for secure AI system development, https://media.defense.gov/2023/Nov/27/2003346994/-1/-1/0/GUIDELINES-FOR-SECURE-AI-SYSTEM-DEVELOPMENT.PDF; World Economic Forum, How to Manage AI Procurement in Public Administration, https://www.weforum.org/agenda/2023/07/how-to-manage-ai-procurement-in-public-administration/

[54] GAO, Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities, https://www.gao.gov/assets/gao-21-519sp.pdf; Center for Inclusive Change, AI Procurement Risk Management Framework, https://www.inclusivechange.org/ai-governance-solutions/rmf-for-ai-procurement

The **National AI Initiative Act** organizes and coordinates federal efforts to promote AI innovation while managing associated risks.[55] Key components include the creation of a National AI Initiative Office to oversee cross-sector AI initiatives, support for a National AI Research Institutes network to drive cutting-edge research, and strategic investments in AI education and workforce development. The Act emphasizes collaboration between academia, industry, and government to establish national standards for AI safety, fairness, and accountability, ensuring that AI technologies benefit society while maintaining public trust. Through this act, the National Institute of Standards and Technology (NIST) was authorized to create a framework for responsible AI governance, promoting standards and guidelines that prioritize public safety, accountability, and transparency.

The **National AI Training Act** mandates that federal employees who work with AI complete a training program covering both AI's technical aspects and societal implications. As part of this mandate, the Government Services Administration (GSA) released its own generative AI-focused training program for federal employees in 2024, ensuring public servants are well-equipped to use and evaluate AI responsibly.[56]

Executive Strategies & Agency Guidance

In 2022, the White House issued its Blueprint for an AI Bill of Rights underscoring fundamental rights such as privacy, transparency, and fairness to protect individuals from AI-related harms and encourage equitable technology use.[57] The White House Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, issued in 2023, is a landmark directive aimed at establishing comprehensive AI safeguards across government and industry.[58] It mandates strict testing and evaluation of AI systems to ensure they align with national security and public safety priorities, including setting guidelines to prevent the misuse of AI in critical sectors such as health, defense, and justice. The order also emphasizes transparency, accountability, and fairness, with a focus on protecting civil rights and privacy through risk assessments and harm reduction strategies. It calls for new standards around algorithmic safety, expanding regulatory and compliance frameworks to mitigate biases and prevent discrimination. The order further seeks to bolster the AI workforce by investing in education, research, and innovation, reinforcing US leadership in safe AI practices. Additionally, it directs federal agencies to prioritize open and secure data-sharing practices, enhancing collaboration with industry and academic partners to responsibly advance AI technology while upholding public trust.

The October 24, 2024, Presidential Memorandum on Advancing US Leadership in Artificial Intelligence (AI) underscores the critical role of AI in strengthening national security and

[55] National Artificial Intelligence Initiative Act of 2020, https://www.congress.gov/bill/116th-congress/house-bill/6216
[56] GSA AI Training, https://coe.gsa.gov/communities/AITraining.html
[57] White House Blueprint for an AI Bill of Rights, https://www.whitehouse.gov/ostp/ai-bill-of-rights/
[58] US White House, Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

safeguarding public interests.[59] This memo directs federal agencies to accelerate the integration of AI to enhance national defense, intelligence, and homeland security, while emphasizing the need for ethical and responsible AI practices. It calls for rigorous testing, evaluation, and oversight mechanisms to ensure AI technologies are safe, reliable, and aligned with democratic values. Agencies are tasked with prioritizing the development of AI systems that uphold transparency, privacy, and accountability, thereby fostering public trust and mitigating risks. The memo also seeks to boost international cooperation in AI, encouraging alliances that support ethical AI use in global security frameworks. Additionally, it aims to bolster the domestic AI workforce through investments in research, education, and workforce training.

Federal agencies have issued detailed guidance to support the safe, transparent, and accountable use of AI. NIST's AI Risk Management Framework (AI RMF) is a cornerstone of these efforts, providing a structured approach for assessing and managing AI risks across various stages, including development, deployment, and monitoring. The AI RMF emphasizes core pillars such as governance, transparency, fairness, and accountability, helping both federal agencies and private sector partners implement AI systems that are both reliable and ethical. NIST's specialized Generative AI Profile further refines these practices, offering a structured approach to managing AI risks, enhancing transparency, and maintaining accountability.[60]

Additionally, the Federal Trade Commission (FTC) has published guidelines aimed at preventing deceptive and unfair practices in AI, particularly emphasizing the need for truthfulness, transparency, and fairness in consumer-facing AI applications.[61] The FTC's guidance warns organizations against the misuse of AI, especially in areas where bias and discrimination could arise, and underscores the importance of consumer consent and data protection. Together, these frameworks and guidelines establish robust expectations for AI governance, ensuring that federal AI applications are designed to foster public trust and align with ethical standards.

Voluntary Commitments

The White House's September 2023 Voluntary AI Commitments outline a set of pledges made by leading AI companies to ensure the safe, secure, and transparent development of advanced AI systems.[62] These commitments, adopted by companies like Google, Microsoft, and OpenAI, focus

---

[59] Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security/

[60] NIST Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, https://airc.nist.gov/docs/NIST.AI.600-1.GenAI-Profile.ipd.pdf

[61] Federal Trade Commission, FTC Authorizes Compulsory Process for AI-related Products and Services, https://www.ftc.gov/news-events/news/press-releases/2023/11/ftc-authorizes-compulsory-process-ai-related-products-services#:~:text=The%20omnibus%20resolution%20will%20streamline,determine%20when%20CIDs%20are%20issued

[62] White House Voluntary Commitments on AI (Sept. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/09/Voluntary-AI-Commitments-September-2023.pdf

on three primary areas: safety, security, and trust. For safety, the companies commit to conducting robust testing and risk assessments to identify and mitigate potential harms from AI, especially those that could pose significant societal risks. In terms of security, the companies pledge to protect model weights and other sensitive information, minimizing risks associated with misuse and unauthorized access. To enhance trust, these commitments emphasize transparency by calling for information-sharing about AI risks, promoting responsible usage, and enabling third-party evaluations and audits of AI models. These voluntary actions signify a collaborative approach between the private sector and government, aimed at establishing a baseline of responsibility and ethics in AI development while maintaining public confidence in these rapidly advancing technologies.

State-Level AI Governance Strategies

Every state has unique features and context, and it will not necessarily be appropriate to apply the same AI governance strategy across the board. However, all states are grappling with how to best ensure their residents enjoy the benefits and avoid the risks associated with AI. There is already a lot to be learned from states' experiences working to govern AI, and greater collaboration and coordination between state and local governments can help facilitate this cross-learning.

The number of AI-related bills and policy action at the state level has increased in recent years. In 2023, around 200 bills were introduced across US states, while in 2024 close to 700 AI-related bills were introduced.[63] Common themes across the bills include a prominent focus on synthetic media and deepfakes; others include information-gathering (e.g., call to establish task forces), preventing algorithmic discrimination, and supporting workforce training. Some of these bills relate to governing the private sector, while others relate to oversight of government AI uses.

A number of notable bills relate to governing the private sector. These are generally out of scope of this report as they do not pertain directly to public sector AI. For reference, examples of these include:

- California's AI Transparency Act, which requires AI providers to disclose AI-generated content.
- California's GenAI Training Data Transparency bill, which requires AI developers to publicly post a high-level summary of the datasets used in the development of the AI system or service.
- Colorado's AI Act, which provides consumer protections against discrimination from high-risk AI systems.[64]
- Utah's AI Policy Act, which requires disclosure of the use of genAI prior to human engagement, and clarifies that companies will be responsible for the statements made by their genAI tools.

[63] 2024 State Summary on AI, https://techpost.bsa.org/2024/10/22/2024-state-summary-on-ai/
[64] Consumer Protections for Artificial Intelligence, https://leg.colorado.gov/bills/sb24-205

More relevant to this report are the examples of **bills to better govern government use of AI** that have been signed into law. US state legislators considered more than 150 bills relating to government use of AI just within the 2024 legislative session.[65] These bills related to creating AI inventories, impact assessments, AI use guidelines, procurement standards, and government oversight bodies.

Notable examples include:

- Vermont's Act relating to the use and oversight of artificial intelligence in State government created a division of Artificial Intelligence to review AI development, use, and procurement, and to inventory all automated decision systems.
- Connecticut's Act Concerning Artificial Intelligence, Automated Decision-Making and Personal Data Privacy requires the Department of Administrative Services to create an inventory of all systems that employ AI and are in use by any state agency, including information about the capabilities and impact assessment of the system, and requires them to perform ongoing assessments of such systems to ensure that none shall result in any unlawful discrimination or disparate impact. The bill also requires the Office of Policy and Management to develop and establish policies and procedures concerning the development, procurement, implementation, utilization and ongoing assessment of systems that employ artificial intelligence and are in use by state agencies.
- California's Bill on an Inventory for High-Risk Automated Decision Systems requires the Department of Technology to develop and maintain a comprehensive inventory of high-risk AI uses developed or procured by state agencies including the categories of data the system uses to make decisions.

In addition to these bills, more than 10 states have issued **executive orders** relating to government use and oversight of AI. The following deepdive on the California executive order on generative AI highlights the role executive orders can play in shaping the use and governance of AI by state governments.

Deepdive: California Executive Order on GenAI

California Governor Gavin Newsom signed Executive Order N-12-23 in September 2023, making California one of the first U.S. states to regulate the use of genAI tools by state agencies.[66] The Executive Order calls upon State agencies to investigate the opportunities and risks of public sector deployment of genAI tools and mandates the development of genAI risk assessments, procurement guidelines, workforce training, and impact assessments.

[65] Artificial Intelligence in Government: The Federal and State Landscape, 2024, https://www.ncsl.org/technology-and-communication/artificial-intelligence-in-government-the-federal-and-state-landscape

[66] California Executive Order on Generative AI, https://www.gov.ca.gov/wp-content/uploads/2023/09/AI-EO-No.12-_-GGN-Signed.pdf

In line with the California Executive Order, the California Department of Technology (CDT), with support from other departments, published the California GenAI Toolkit in March 2024.[67] This toolkit serves as a centralized hub for hosting guidelines and resources mandated by the Executive Order for state staff on procurement, workforce training, and the use of genAI tools by state agencies. This toolkit is a living document that is continuously updated with new state guidance as it becomes available. Additional guidelines are expected to be added to the toolkit over time. For example, all state entities are required to submit an inventory of all high-risk use cases of genAI by state entities to CDT for the creation of a state-wide inventory. Guidance for genAI inventory reporting will be posted to the toolkit once finalized.

The Executive Order directed state agencies to develop guidelines and establish a specialized procurement process for genAI tools, distinct from standard procurement procedures.[68] The new guidelines outline procurement workflows for two different scenarios: (1) new contracts in which genAI tools are deliberately acquired at the outset of the procurement process, and (2) new contracts in which genAI tools are later identified upon disclosure notification by the vendor. Guidance on genAI disclosures from vendors with existing contracts is still under development.

Effective April 2024, vendors making a bid to state agencies are required to include a genAI disclosure notification clause verbatim in all proposals and contracts.[69] This clause mandates that bidders disclose in writing if their service incorporates any genAI technology, including from third party vendors. Failure to disclose will result in a voided contract. Additionally, bidders must complete a GenAI Disclosure & Factsheet in order to be eligible for a state contract. This document requires detailed disclosures on the genAI model, training data, inputs and outputs, performance metrics, bias assessments—among other details.

Effective July 2024, state entities must first conduct a risk assessment for all new genAI procurements and acquisitions under consideration to determine their associated level of risk. To enable this, CDT produced a Generative Artificial Intelligence Risk Assessment (SIMM 5305-F) form which all state entities must complete to evaluate the risks associated with proposed genAI projects.[70] The assessment requires state entities to assign a risk level—High, Moderate, or Low—based upon criteria outlined in the form. The assessment is based on two factors: the type of information involved (i.e., sensitivity of data and associated risk of unauthorized access) and the expected use of the data (i.e., potential risks of relying on genAI outputs for State decision-making, tasks, and services). For genAI systems rated as Moderate or High risk, a designated genAI subject matter expert within the department must consult with CDT to assess and mitigate risks. This involves co-creating a risk mitigation plan and providing additional details regarding the vendor and state agencies' planned transparency practices, human oversight, and equity measures.

[67] GovOps, GenAI Toolkit, https://www.govops.ca.gov/wp-content/uploads/sites/11/2024/03/GenAI-Toolkit-004.pdf
[68] California Department of Technology Procurement Guidance, https://genai.cdt.ca.gov/procurement/
[69] California Department of Technology Contract Disclosure and Special Provisions, https://genai.cdt.ca.gov/procurement/contract-disclosure-and-special-provisions.html
[70] California Department of Technology, Generative AI Risk Assessment, https://cdt.ca.gov/wp-content/uploads/2024/03/SIMM-5305-F-Generative-Artificial-Intelligence-Risk-Assessment-FINAL.pdf

The Executive Order further requires state agencies to make genAI workforce training available to state employees to support the safe, secure, and responsible deployment of the technology. The toolkit hosts information on phased workforce training recommended for state staff.[71] This guidance contains a summary of recommended genAI training modules based upon staff level, encompassing genAI risk mitigation and technical training. The toolkit recommends a "phased approach" to workforce training, in which executives and legal, labor, and privacy specialists receive training first. The California Department of Human Resources (CalHR) is developing a general course on genAI for all levels of state staff that will eventually be added to the toolkit.

Section 7. Strategic Roadmap for AI Implementation & Oversight

Implementing a responsible AI governance strategy is crucial for ensuring that AI applications in the public sector align with existing policies, directives, Executive Orders, and strategic goals. This framework should include:

- **Alignment with Existing Policies and Directives:** Conduct a thorough analysis to ensure that the strategy adheres to existing national and state-level policies, including directives and Executive Orders that outline ethical and operational requirements for AI use.
- **Initial Procurement and Use Guidelines:** Develop clear guidelines for the procurement and implementation of AI technologies, prioritizing transparency, accountability, and inclusivity. These guidelines should specify:
    - Criteria for evaluating AI technologies based on ethical considerations, technical robustness (including safety and security measures), and alignment with public interest objectives.
    - Mechanisms for ongoing monitoring and auditing to assess the impact and performance of AI systems post-implementation.
- **Monitoring and Evaluation:** Establish processes for continuous evaluation of AI applications to ensure compliance with legal, ethical, and performance standards.
- **Integration:** Map and connect your strategy to other AI policy efforts, such as statewide AI task forces, automated decision systems governance, and inter-agency collaborations, ensuring consistency and a unified approach across the public sector. Resources, such as training, software and hardware, should be shared to support statewide adoption.
- **Looking Over the Horizon**: Understand shifts in AI technological development to prepare for new capabilities, risks, and impacts.

Short-Term Goals (6 months)

In the immediate term, public sector entities should focus on foundational steps to assess the appropriateness of AI applications and establish a framework for responsible integration:

[71] California Department of Technology AI Training and Resources, https://genai.cdt.ca.gov/training-and-resources/

- **Oversight Body:** Designate an entity(ies) to guide the statewide approach to adoption and use of AI
    - **Policy Development & Alignment**: Designated entity(ies) can develop and align policies that address pressing AI challenges, such as bias mitigation, data privacy, and interoperability with existing systems.
- **Pilot Projects:** Launch small-scale pilot projects to test the feasibility, efficacy, and risks of AI technologies in specific government functions, such as public service delivery or resource management.
- **Sandboxes:** Create controlled environments for testing AI applications under real-world conditions, allowing for iterative learning while minimizing risks.
- **Collaboration & Support:** Designated entity(ies) should engage with state and national associations to facilitate information sharing and operational efficiencies, such as the National Association of State Technology Directors (NASTD), the National Governors Association (NGA), and the Center for Public Sector AI (CPSAI).[72]

Medium-Term Goals (1-2 years)

Building on short-term efforts, public sector entities should aim to responsibly scale AI applications and expand their use to new domains if appropriate:

- **Scaling AI Initiatives:** Transition from pilot projects to full-scale implementations in areas such as healthcare, education, and public safety, while maintaining rigorous oversight mechanisms.
- **Capacity Building:** Invest in training and upskilling public sector employees to manage and evaluate AI systems effectively.
- **Collaborative Frameworks:** Foster partnerships with academia, industry, and civil society to co-create AI solutions that address public needs and enhance governance capacity.

Long-Term Vision (2+ years)

A long-term vision for responsible AI governance focuses on institutionalizing values and ensuring sustainable and ethical AI adoption:

- **AI Driven by Values:** Embed principles of equity, accountability, and transparency into AI governance and operations within government.
- **Operationalizing Governance Strategies:** Develop advanced technical and governance frameworks that facilitate seamless integration of AI technologies, ensuring they enhance public services without compromising ethical and technical standards.

[72] National Association of State Technology Directors, National Governors Association,https://www.nastd.org/home; https://www.nga.org/; Center for Public Sector AI, https://www.cpsai.org/

- **Ongoing Innovation and Adaptation:** Create flexible governance and oversight mechanisms that enable continuous adaptation and adoption of emerging AI technologies, ensuring adoption is relevant, effective, and timely.

Washington's Strategy

WaTech, Washington's statewide technology agency, guides the state's IT strategy and enterprise architecture. WaTech is leading the integration of genAI technology into Washington state operations by aligning efforts with existing policies and directives, developing procurement guidelines; establishing monitoring and evaluation processes, including through the development of sandboxes; integrating AI development and governance efforts across agencies; including sharing resources and infrastructure.

WaTech published its strategic plan in its "State of Washington Generative Artificial Intelligence Report." A high-level summary of the plan and timeline are included below.[73]

Strategic Plan & Timeline

Phase 1 (first 6 months)	- Development of WaTech's role in guiding the statewide approach to genAI adoption, including its role as a broker between agencies - Development of a phased, iterative approach to deploying genAI - Expansion of governance strategies, shared services and resources, and support
Phase 2 (6 months)	- Identification of genAI use cases through its Emerging Technology and Innovation and Modernization Programs - Integration of genAI into existing statewide services - Collaborate with agencies seeking to implement genAI - Test and deploy the secure sandbox
Phase 3 (6-12 months)	- Expand genAI projects through the Innovation and Modernization Program - Solidify the Emerging Technologies Program as a coordinating function for continuous support and feedback, enabling usage, scaling, and robust performance
Long-Term (1-2 years)	The Emerging Technology and Innovation and Modernization Programs will be leveraged to support: - Continuous improvement in technological advancements - Development of genAI applications aligned with and effective with state needs

[73] WaTech, Sept. 2024, State of Washington Generative Artificial Intelligence Report, https://watech.wa.gov/sites/default/files/2024-10/WA_State_GenAIReport_FINAL.pdf

Appendix A. Methodology

UC Berkeley, in collaboration with WaTech, conducted a survey of Washington State and local government agencies to identify the opportunities and barriers to the development and implementation of artificial intelligence (AI) tools, including generative AI, in their workflows. This survey aimed to collect data on the current use of AI in government, employee perceptions of its benefits and risks, and to evaluate the need for guidance, training, and governance.

UC Berkeley collaborated with WaTech to design the survey and distributed it using Qualtrics survey software. The survey was open from April to June 2024 and comprised 19 optional questions, estimated to take 10 to 15 minutes to complete. Approximately 200 individuals viewed or partially filled out the survey, but only those who submitted complete responses were included in the final analysis. After completing our data cleaning procedures, 131 valid responses were retained. UC Berkeley anonymized the dataset and chose to keep individual survey responses confidential by only sharing aggregated results publicly.

We took a mixed-methods approach for the survey analysis, employing both quantitative and qualitative techniques to analyze the response data. Because all questions were optional, the number of responses varied per question, and when relevant, response count was indicated on the corresponding data visualizations.

Appendix B. Survey Questions

1. What organization do you work within?

2. Which type of work best describes your role?
    - Executive
    - Manager
    - Staff
    - Other:

3. Do people within your organization use any kind of AI technologies for official work purposes? [Yes, No, Unsure]

4. If yes, what AI-enabled tools are people using? [Select all that apply]
    - Predictive analytics
    - Image recognition
    - Machine learning
    - Large language models / generative AI
    - Other (please specify)

5. If yes, please describe the particular use cases if you can.

6. If yes, how does the organization monitor and track the effectiveness of the AI technologies in use? [Select all that apply]
    - Continuous monitoring tool or service
    - Incident reporting
    - Quarterly reviews
    - Annual reviews
    - There is no systematic process to monitor and track effectiveness
    - Other (please specify)

7. What do you think are the best use cases and greatest **benefits** of using AI within your organization? [Select all that apply]
    - Summarizing content
    - Analyzing data
    - Detecting images
    - Giving predictions
    - Assistance with writing drafts or refining written text
    - Assistance with writing code
    - Generating images
    - Generating audio
    - Generating video
    - Translating languages
    - An AI chatbot
    - Other (please specify)

8. What do you think are the biggest **risks**, challenges, and concerns associated with using AI within your organization? [Select all that apply]
    - Privacy risks related to the use of PII or sensitive state data
    - Security risks related to AI vulnerabilities
    - Equity concerns relating to biased or discriminatory inputs or outputs
    - Copyright and fair use concerns related to AI training data
    - Labor rights concerns related to the potential automation of jobs
    - Accuracy and reliability concerns
    - Potential for misuse
    - Environmental impact
    - Other (please specify)

9. Does your organization have any **AI policies** in place? If so, what are they and who developed them (e.g. privacy office, security office, CIO, etc)?

10. What additional guidance, if any, would you like to see to support responsible **procurement** of AI technologies within your organization? [Select all that apply]

- Examples of acceptable and unacceptable use cases
- A new AI vendor assessment process
- An AI tool assessment process
- An AI vendor list
- Other (please specify)

11. Do you think that existing **privacy and security reviews** should be amended to address unique characteristics of AI systems? If so, how?

12. Ideally, what would a more comprehensive **AI risk assessment** look like? What should be included in the assessment? What do you think the process should look like?

13. Ideally, what would a more comprehensive **AI impact, equity, and bias assessment** look like? What should be included in the assessment(s)? What do you think the process should look like?

14. What features or contexts of use do you think should contribute to an AI system being classified as **high risk** or unacceptable risk? [Select all that apply]
    - If the system will be used in a high risk domain
    - If the system will be prone to malicious use
    - If the system uses sensitive data
    - If the system is particularly prone to error or hallucination
    - If the system is expected to work significantly less well for certain groups
    - If the system is easily manipulated and introduces significant security risks
    - If the system is extremely high cost
    - If the system is likely to significantly alter or replace jobs
    - Other (please specify)

15. Do you think there are any impacts of AI on the **state workforce**? If yes, what do you think the greatest impacts will be? [Select all that apply]
    - AI tools are likely to significantly improve the efficiency and effectiveness of the state workforce
    - AI tools are likely to augment the tasks that people carry out
    - AI tools are likely to fully automate some current jobs
    - AI tools are likely to change the way most people in the state workforce carry out their work
    - Other (please specify)

16. Do you think additional resources or **training** within your organization on how to use AI including responsible practices would be helpful? If so, what types? Do you think these should be integrated into existing training or be separate?[Select all that apply]
    - Training on different AI technologies and how they can be used

- Training on responsible AI (privacy, security, safety, ethics)
- Training on how to validate an AI tool
- Training on how to validate the accuracy and equity of AI-generated content
- Training on how to implement an AI-enabled tool into existing processes
- Training on how to communicate about AI tools to communities you serve
- Training that touches on all of the above
- Other (please specify)

17. Do you think it would be helpful if your organization had "Responsible AI Champions" who could help provide guidance to others? [Yes, No, Maybe]

18. What forms of guidance and support would you want to see from an internal and external statewide community of AI professionals?

19. What information about AI used across the state would be helpful to include in an **inventory**? What information about AI used across the state should be made public?

Appendix C. Results Summary

We identified several key themes from the survey results, including the following:

1. Many people are using AI tools already in their work, and especially generative AI tools
2. People want clarity and guidance about acceptable uses and how to document, disclose, and monitor their uses
3. There is a lot of uncertainty and disagreement about how much impact these tools will have on people's jobs and whether they will help or hinder their core missions
4. People are generally eager to have more training including both high level training on AI and how to use it responsibly as well as very targeted training depending on their role
5. People generally want to see a lot more transparency and accountability from AI vendors
6. People generally expect significant transparency from the state government about its uses, testing, and governance of AI tools

Appendix D. Figures

Figure 1

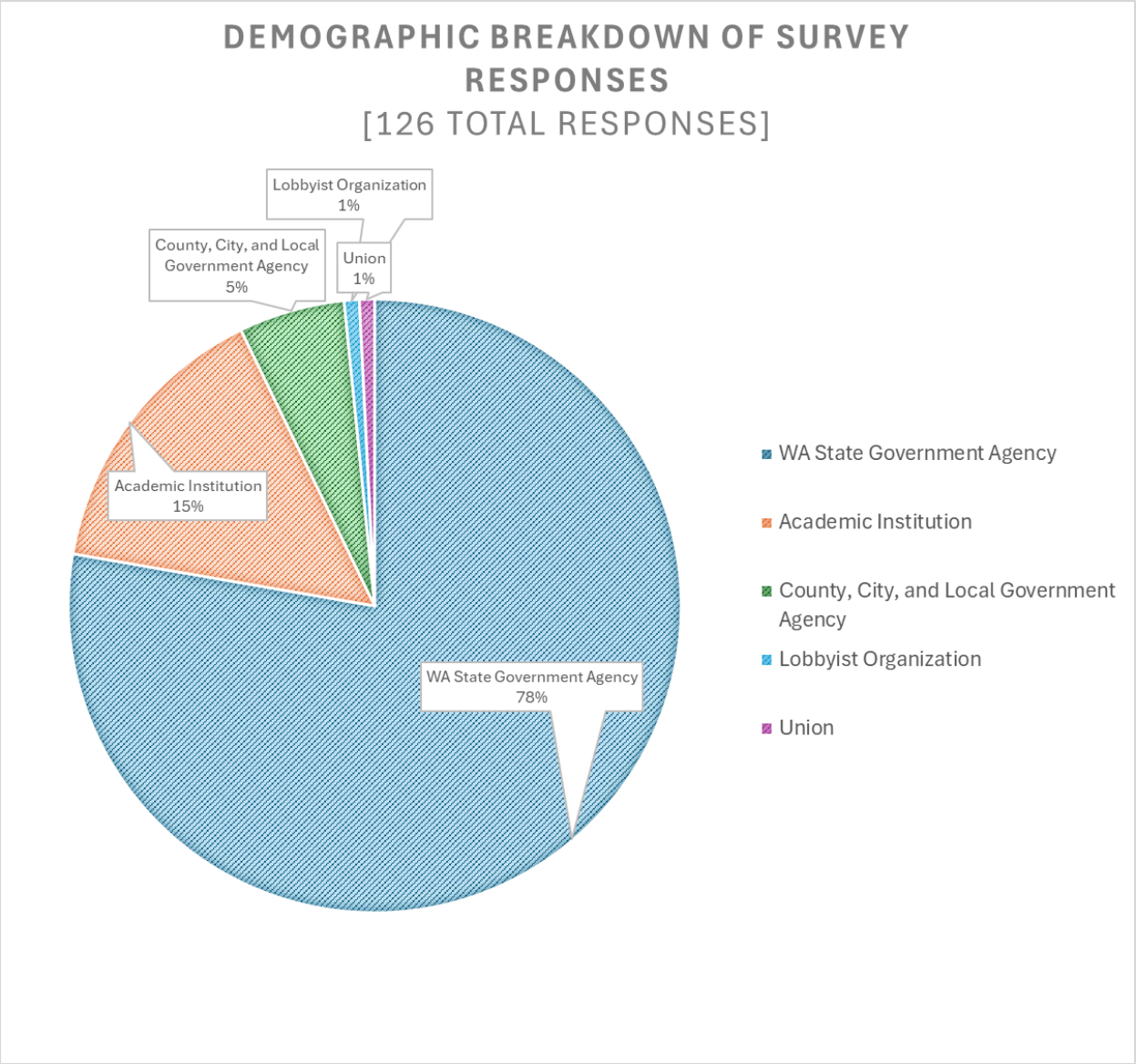


Figure 2

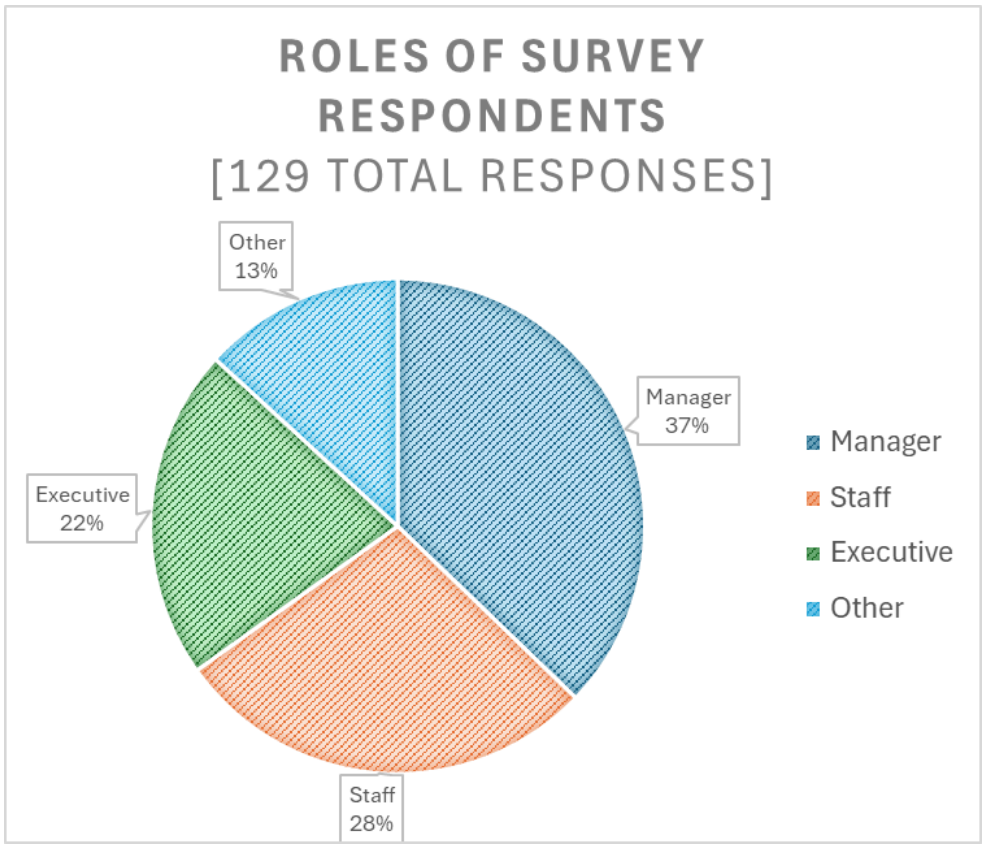

ROLES OF SURVEY RESPONDENTS
[129 TOTAL RESPONSES]
Other 13%
Manager 37%
Executive 22%
Staff 28%
Manager
Staff
Executive
Other

Figure 3

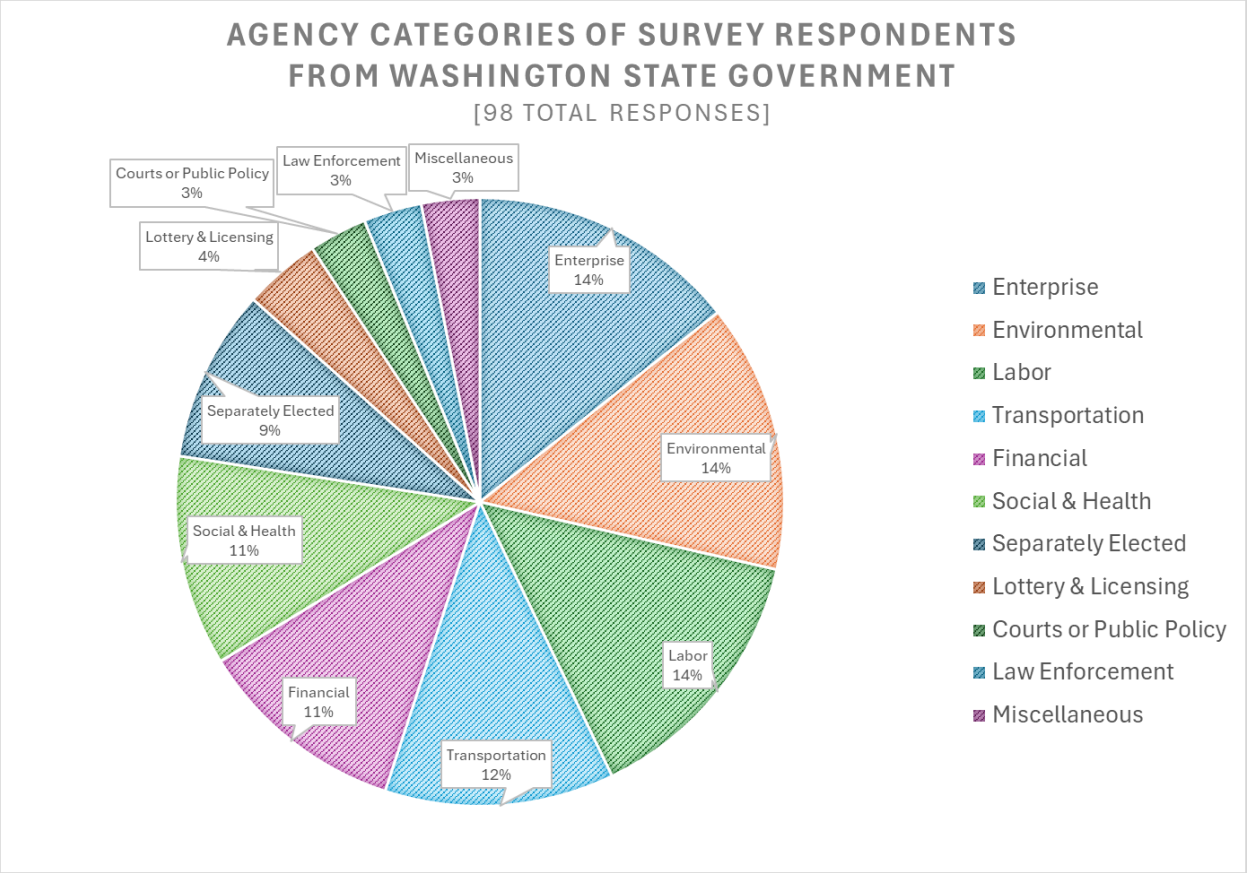

AGENCY CATEGORIES OF SURVEY RESPONDENTS
FROM WASHINGTON STATE GOVERNMENT
[98 TOTAL RESPONSES]
Enterprise 14%
Environmental 14%
Labor 14%
Transportation 12%
Financial 11%
Social & Health 11%
Separately Elected 9%
Lottery & Licensing 4%
Courts or Public Policy 3%
Law Enforcement 3%
Miscellaneous 3%
Enterprise
Environmental
Labor
Transportation
Financial
Social & Health
Separately Elected
Lottery & Licensing
Courts or Public Policy
Law Enforcement
Miscellaneous

Figure 4

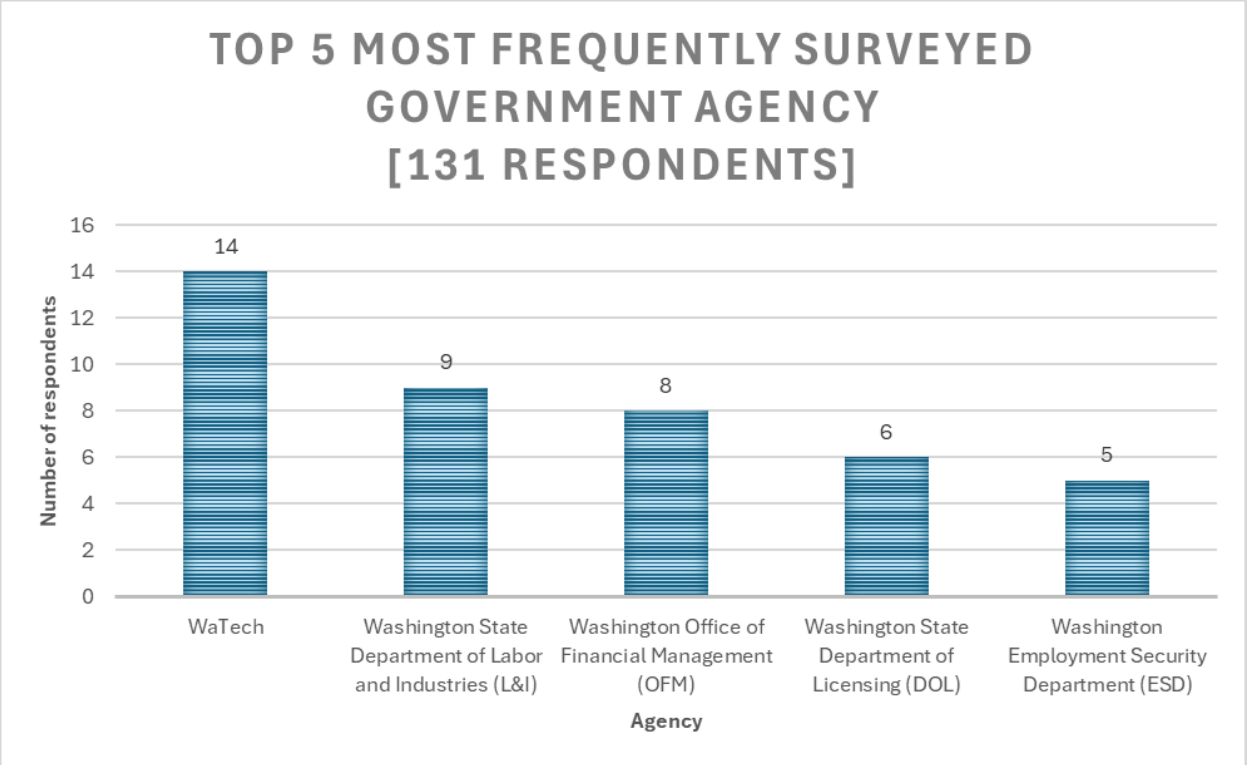

TOP 5 MOST FREQUENTLY SURVEYED GOVERNMENT AGENCY [131 RESPONDENTS]
Number of respondents
16
14
12
10
8
6
4
2
0
14
9
8
6
5
WaTech
Washington State Department of Labor and Industries (L&I)
Washington Office of Financial Management (OFM)
Washington State Department of Licensing (DOL)
Washington Employment Security Department (ESD)
Agency

Figure 5

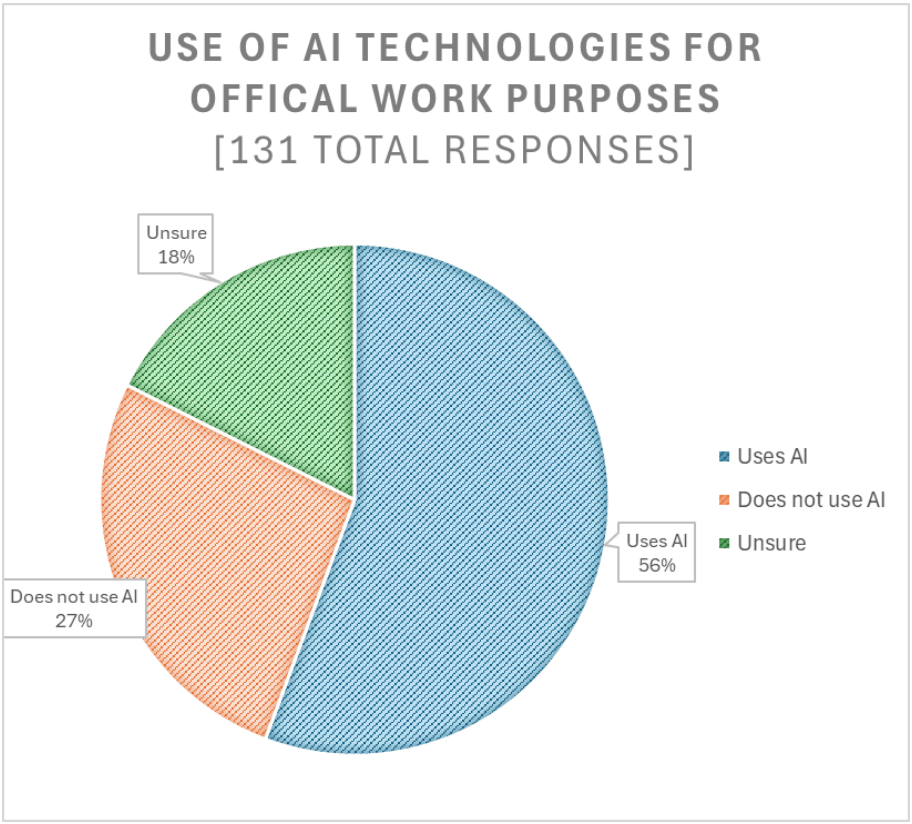

USE OF AI TECHNOLOGIES FOR OFFICAL WORK PURPOSES
[131 TOTAL RESPONSES]
Unsure 18%
Uses AI 56%
Does not use AI 27%
Uses AI
Does not use AI
Unsure

Figure 6

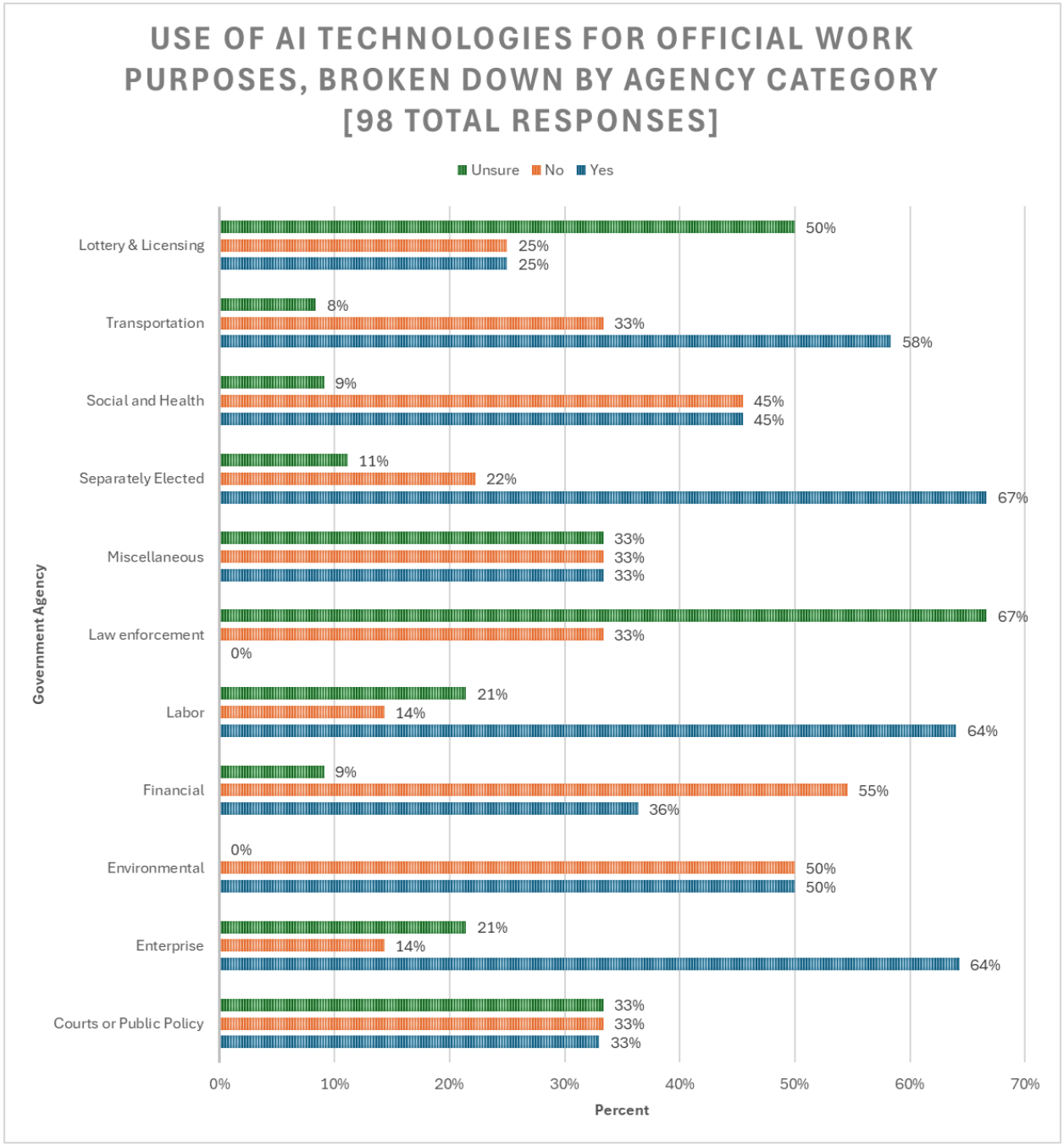

USE OF AI TECHNOLOGIES FOR OFFICIAL WORK PURPOSES, BROKEN DOWN BY AGENCY CATEGORY [98 TOTAL RESPONSES]
Unsure
No
Yes
Government Agency
Lottery & Licensing
50%
25%
25%
Transportation
8%
33%
58%
Social and Health
9%
45%
45%
Separately Elected
11%
22%
67%
Miscellaneous
33%
33%
33%
Law enforcement
67%
33%
0%
Labor
21%
14%
64%
Financial
9%
55%
36%
Environmental
0%
50%
50%
Enterprise
21%
14%
64%
Courts or Public Policy
33%
33%
33%
0%
10%
20%
30%
40%
50%
60%
70%
Percent

Figure 7

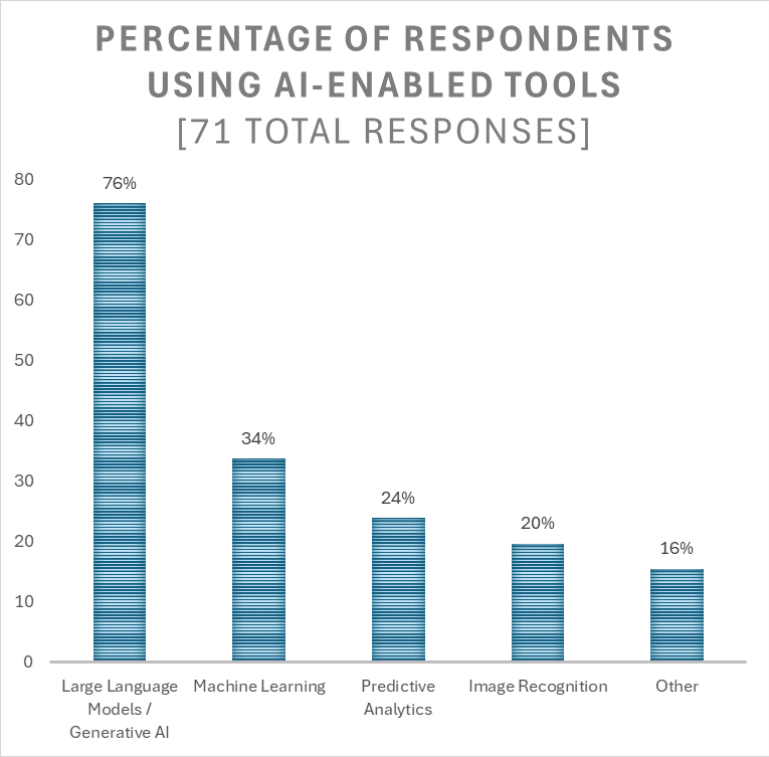

PERCENTAGE OF RESPONDENTS USING AI-ENABLED TOOLS
[71 TOTAL RESPONSES]
80
70
60
50
40
30
20
10
0
76%
34%
24%
20%
16%
Large Language Models / Generative AI
Machine Learning
Predictive Analytics
Image Recognition
Other

Figure 8

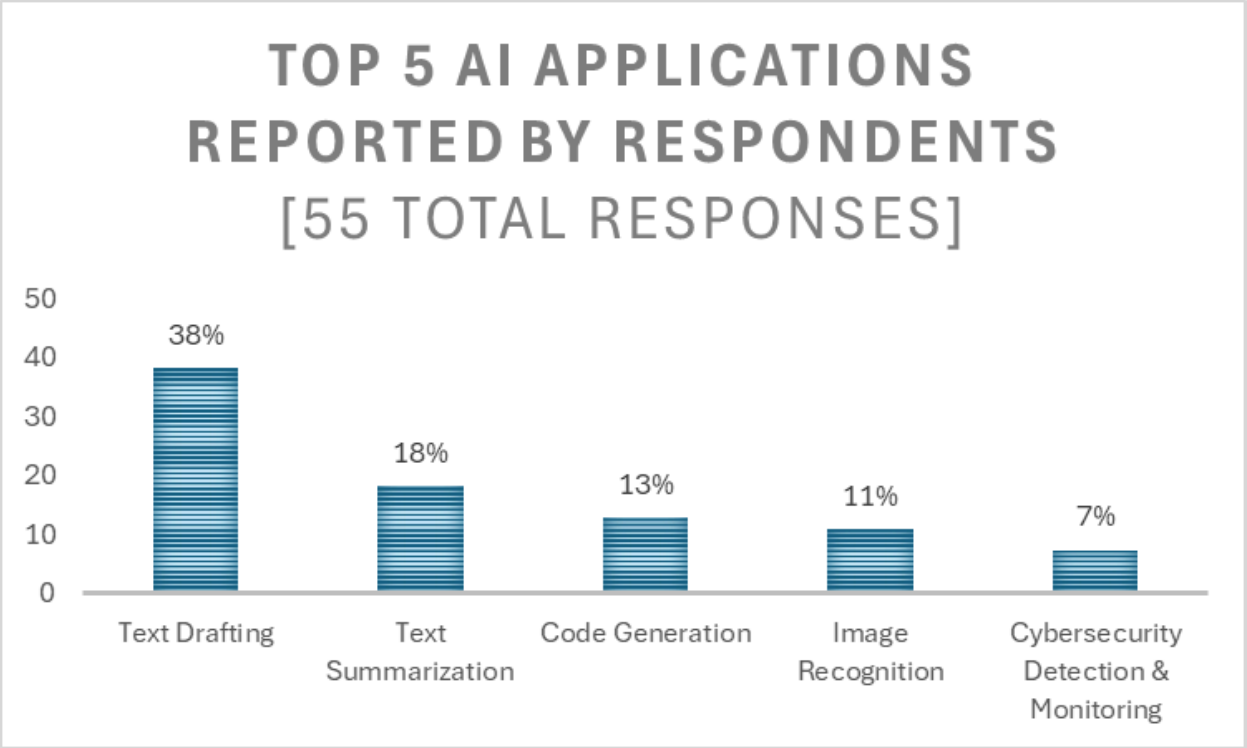


Figure 9

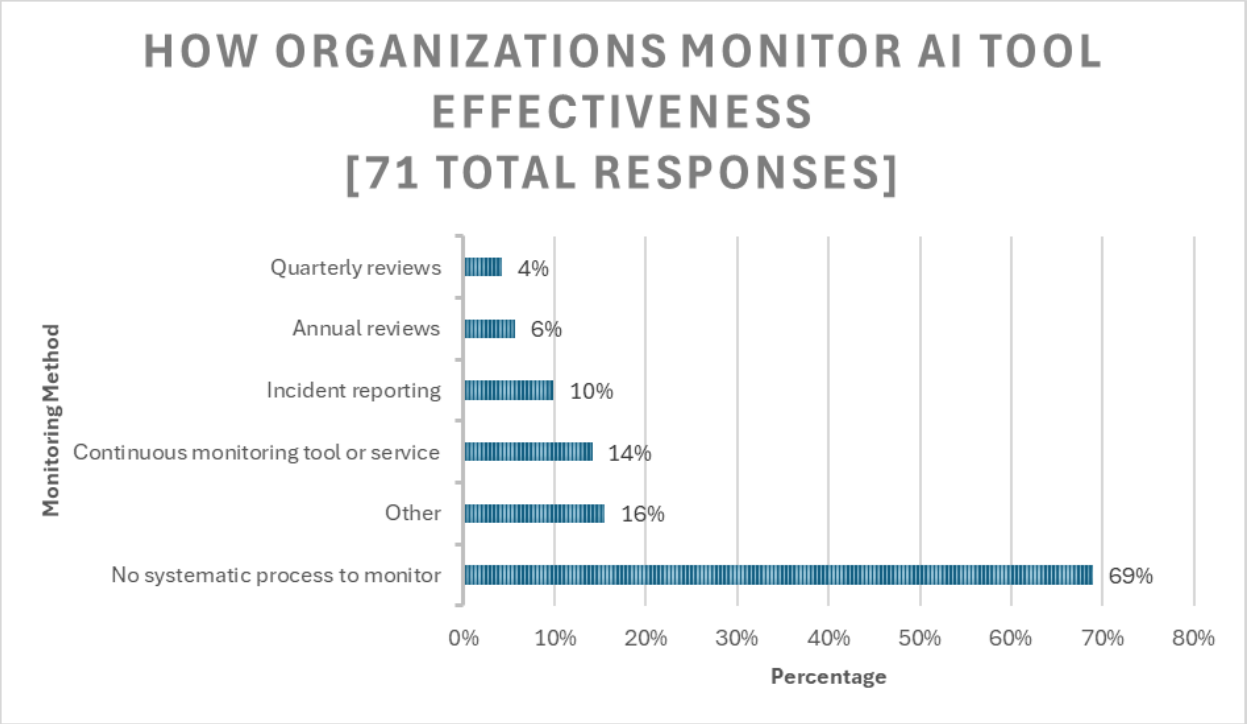


Figure 10

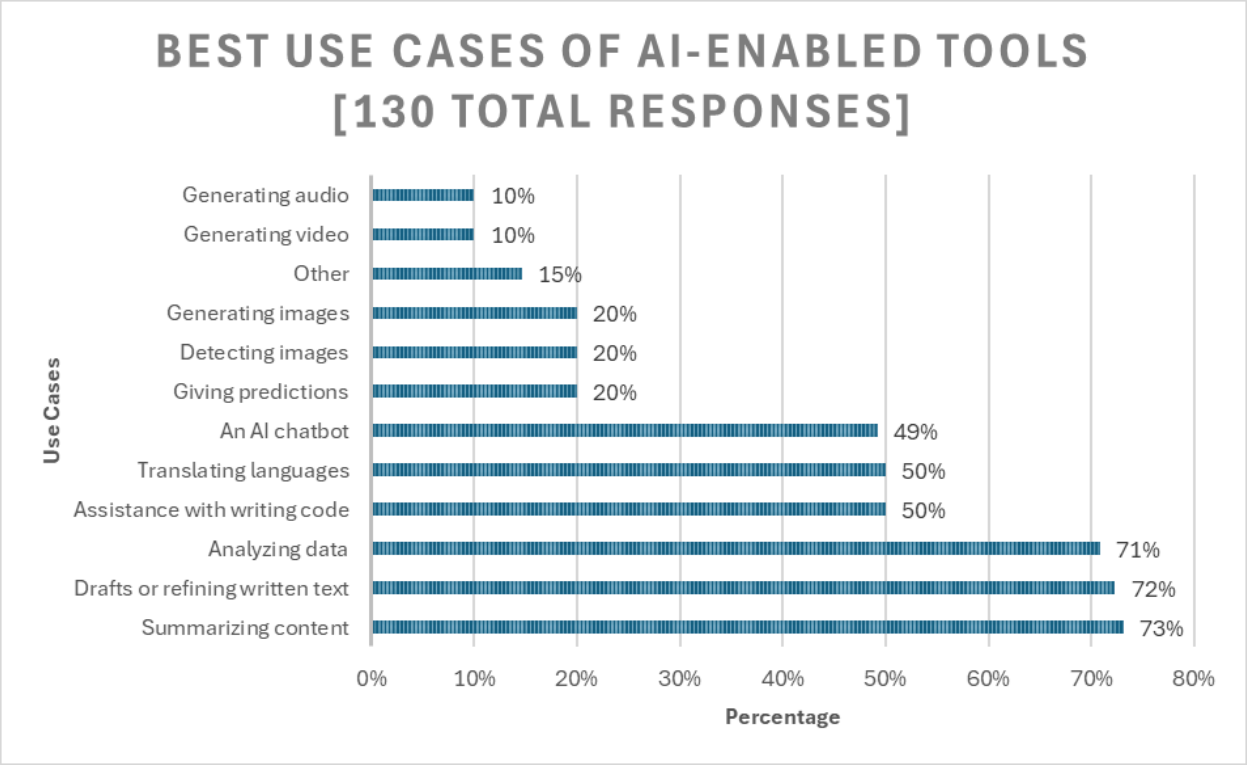


Figure 11

Most Frequently Indicated Best Use Case of AI tools, Segmented by Repondent Job Position					
Role	**Frequency Rank #1**		**Frequency Rank #2**		**Frequency Rank #3**
Executives (n = 28)	Drafts or refining written text (82.1%)	Summarizing Content (82.1%)	Analyzing Data (78.6%)		Translating languages (57.1%)
Managers (n = 48)	Summarizing Content (70.8%)		Drafts or refining written text (68.8%)	Analyzing data (68.8%)	An AI chatbot (47.9%)
Staff (n = 36)	Analyzing data (75%)		Summarizing Content (72.2%)	Drafts or refining written text	Assistance with writing code (61.1%)


(72.2%)

Figure 12

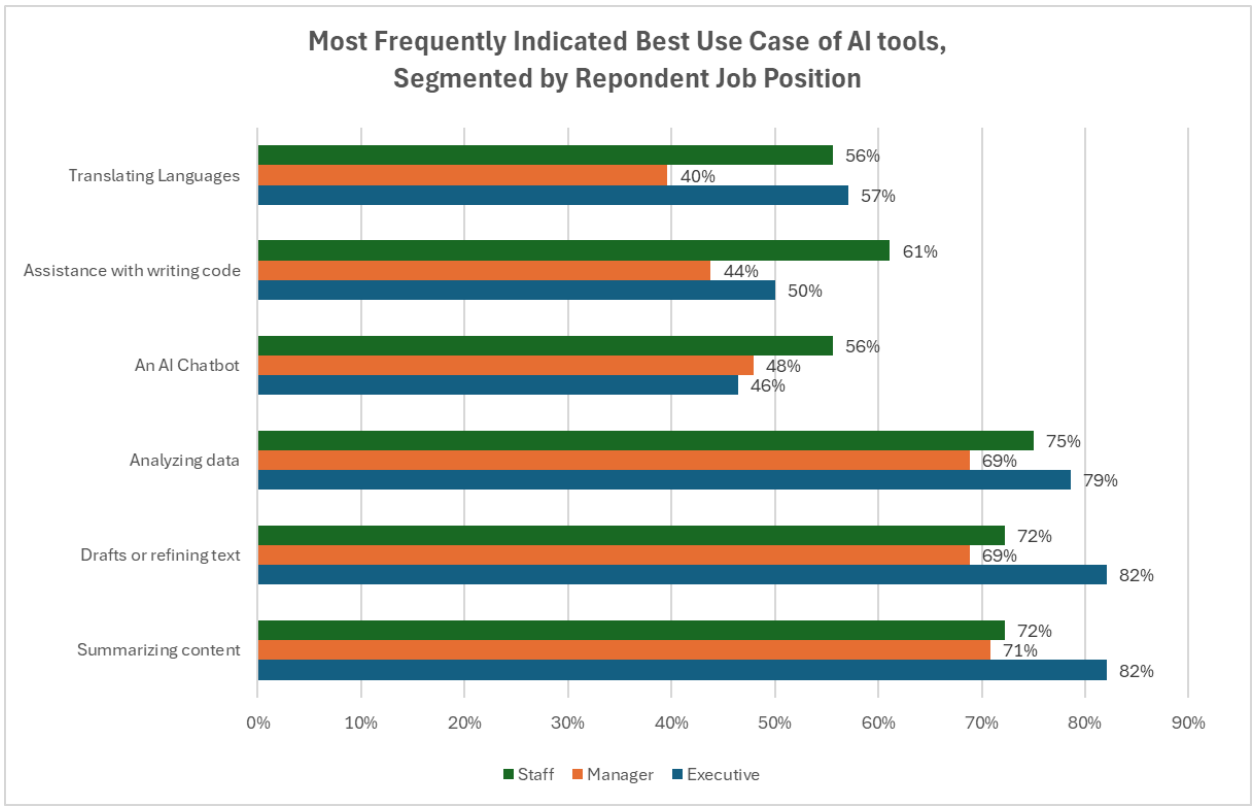


Figure 13

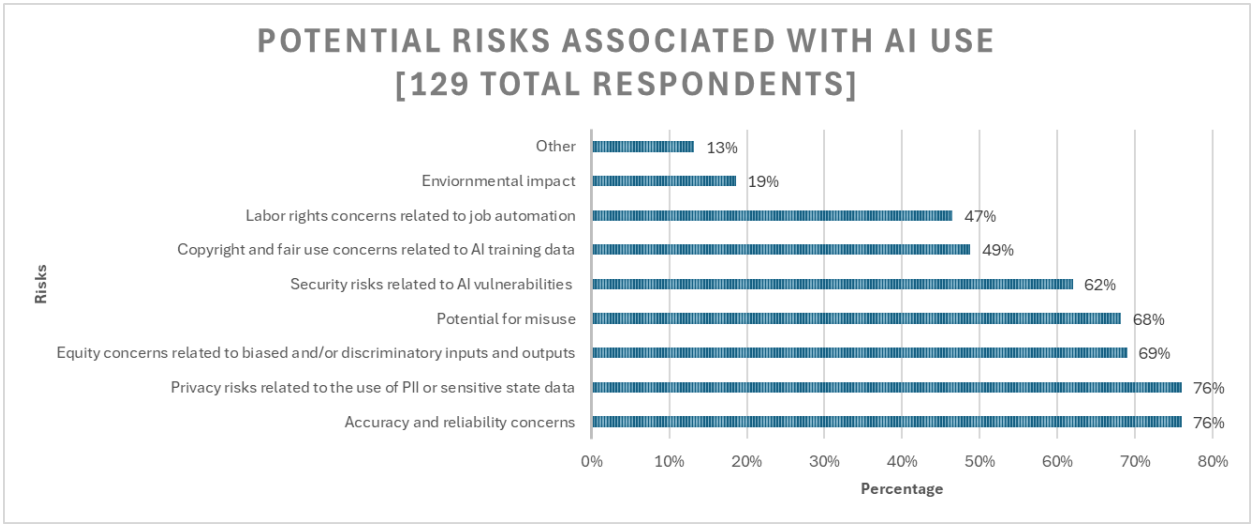


Figure 14

Most Frequently Indicated Potential Risks associated with AI use, Segmented by Respondent Job Position				
Role	**Frequency Rank #1**	**Frequency Rank #2**		**Frequency Rank #3**
Executives (n = 28)	Accuracy and reliability concerns (75%)	Equity concerns relating to biased or discriminatory inputs or outputs (71.4%)	Security risks related to AI vulnerabilities (71.4%)	Potential for misuse (67.9%)
Managers (n = 48)	Accuracy and reliability concerns (83.3%)	Privacy risks related to the use of PII or sensitive state data (77.1%)		Security risks related to AI vulnerabilities (72.9%)
Staff (n = 36)	Privacy risks related to the use of PII or sensitive state data (77.8%)	Accuracy and reliability concerns (75%)		Equity concerns relating to biased or discriminatory inputs or outputs (66.7%)

Figure 15

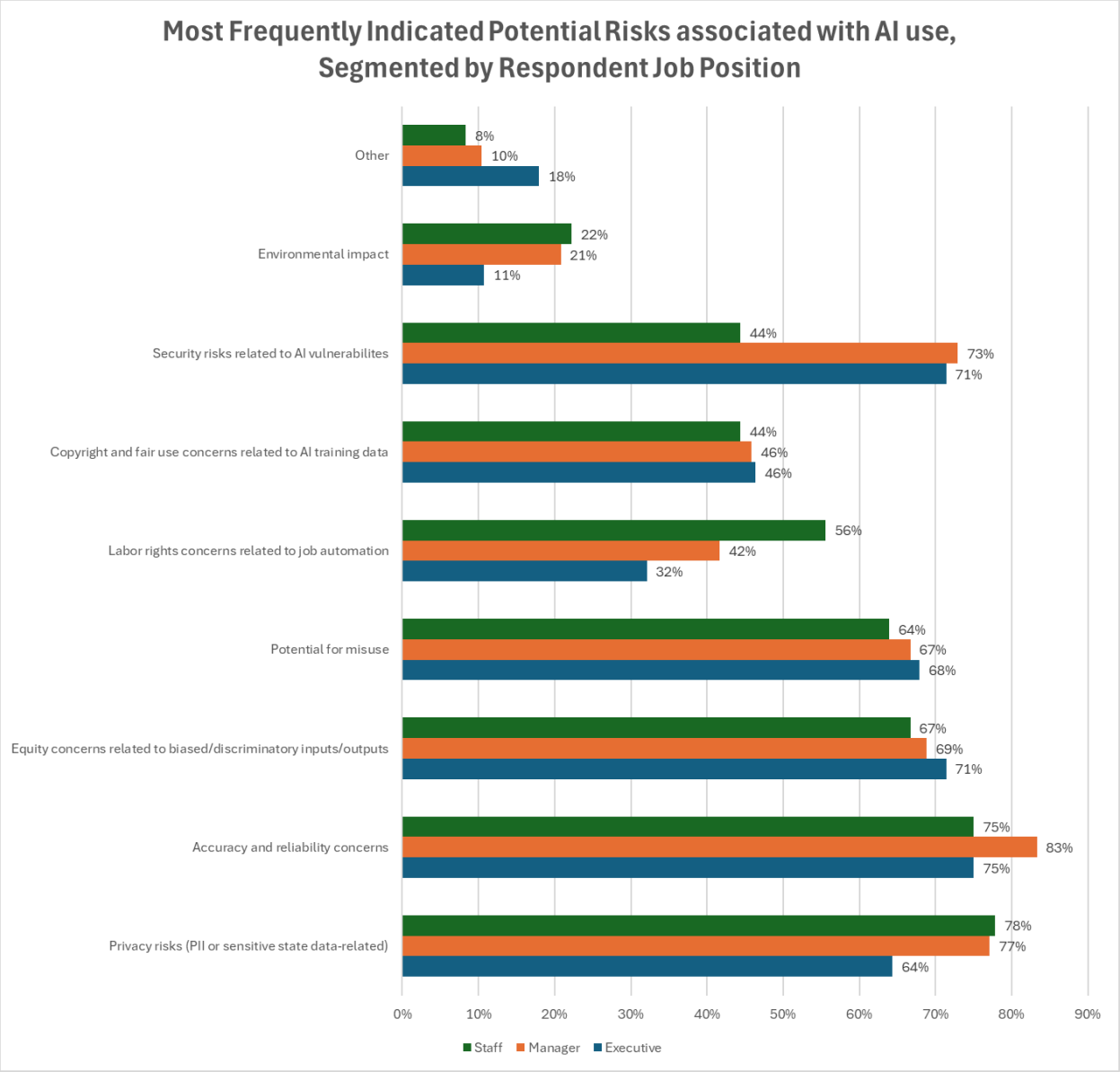

Most Frequently Indicated Potential Risks associated with AI use, Segmented by Respondent Job Position
Other
8%
10%
18%
Environmental impact
22%
21%
11%
Security risks related to AI vulnerabilites
44%
73%
71%
Copyright and fair use concerns related to AI training data
44%
46%
46%
Labor rights concerns related to job automation
56%
42%
32%
Potential for misuse
64%
67%
68%
Equity concerns related to biased/discriminatory inputs/outputs
67%
69%
71%
Accuracy and reliability concerns
75%
83%
75%
Privacy risks (PII or sensitive state data-related)
78%
77%
64%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
Staff
Manager
Executive

Figure 16

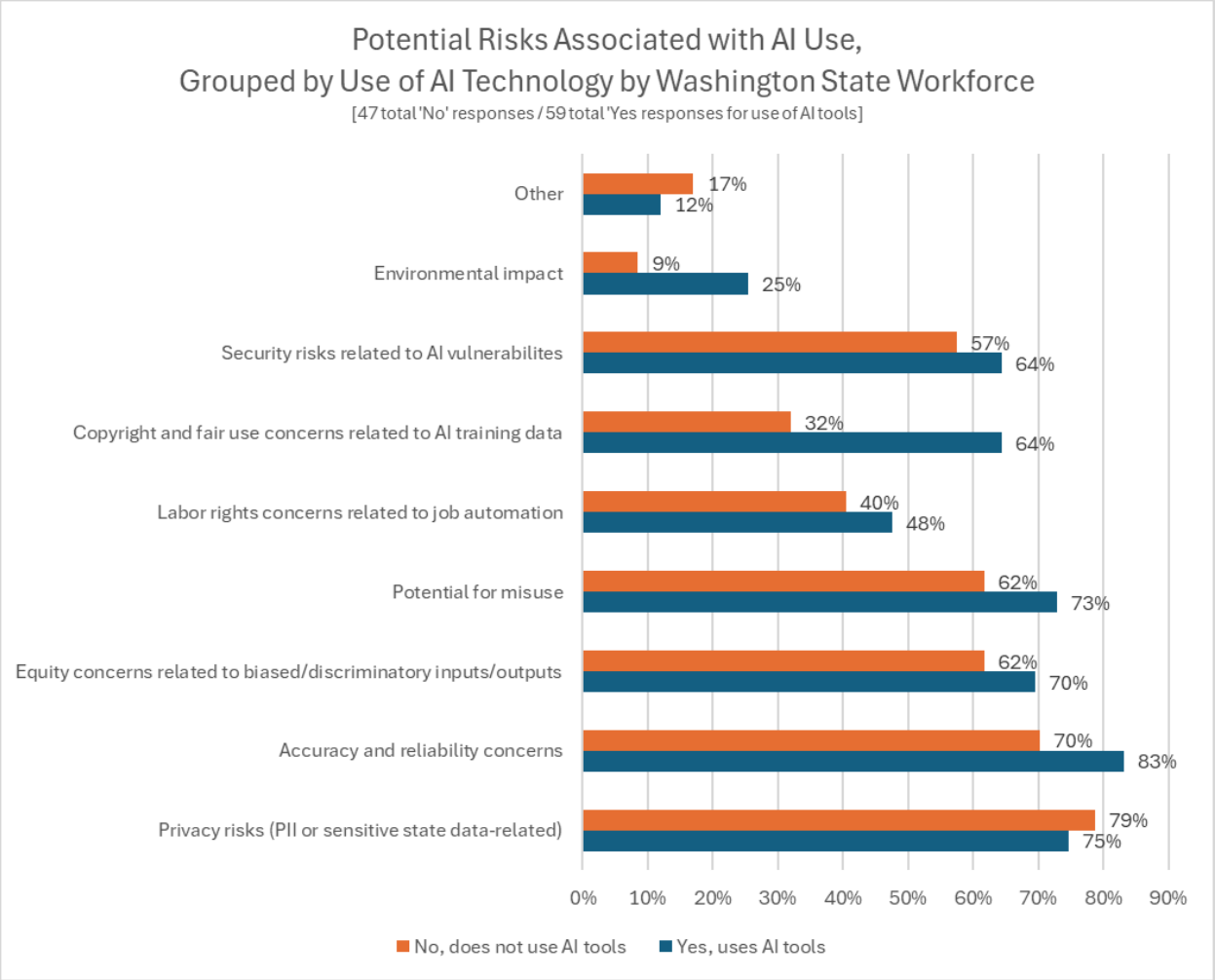

Potential Risks Associated with AI Use,
Grouped by Use of AI Technology by Washington State Workforce
[47 total 'No' responses / 59 total 'Yes responses for use of AI tools]
Other
17%
12%
Environmental impact
9%
25%
Security risks related to AI vulnerabilites
57%
64%
Copyright and fair use concerns related to AI training data
32%
64%
Labor rights concerns related to job automation
40%
48%
Potential for misuse
62%
73%
Equity concerns related to biased/discriminatory inputs/outputs
62%
70%
Accuracy and reliability concerns
70%
83%
Privacy risks (PII or sensitive state data-related)
79%
75%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
No, does not use AI tools
Yes, uses AI tools

Figure 17

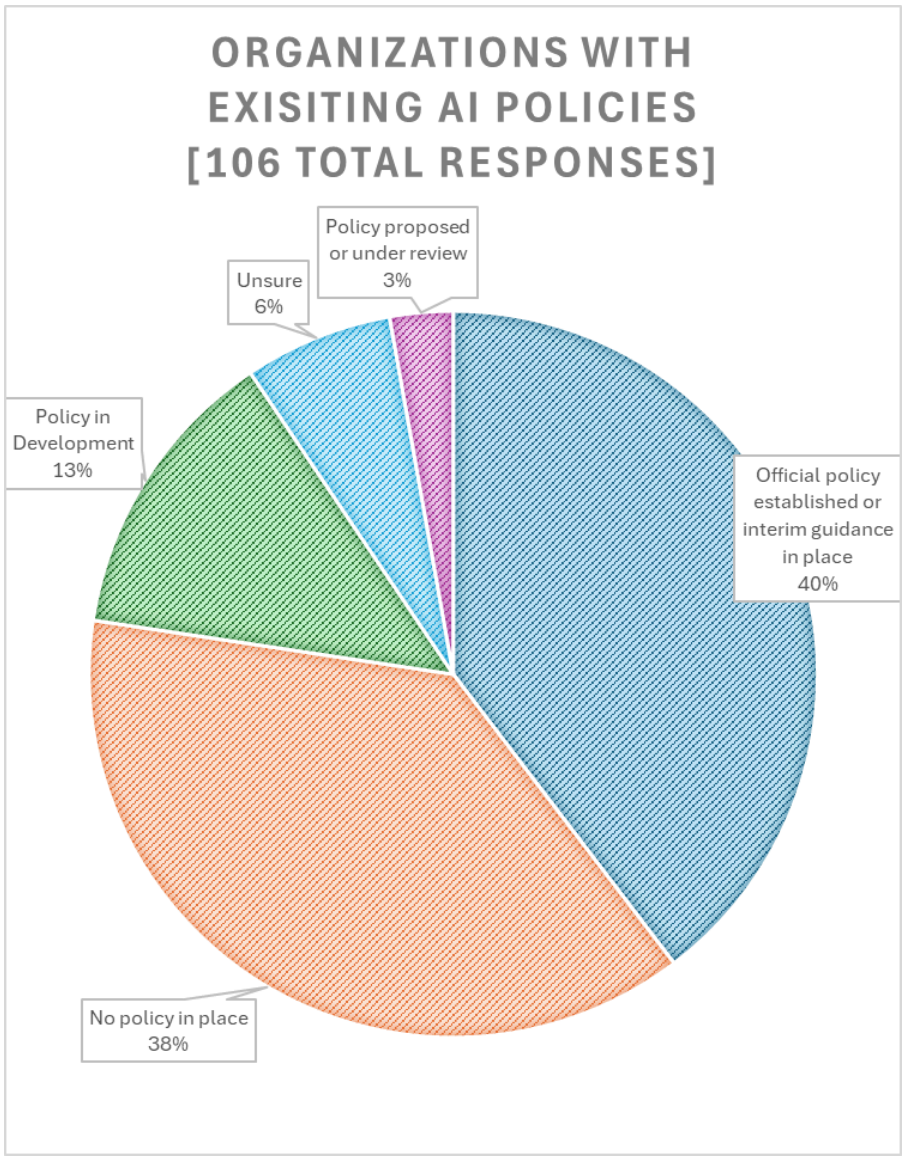

ORGANIZATIONS WITH EXISITING AI POLICIES [106 TOTAL RESPONSES]
Policy proposed or under review 3%
Unsure 6%
Policy in Development 13%
Official policy established or interim guidance in place 40%
No policy in place 38%

Figure 18

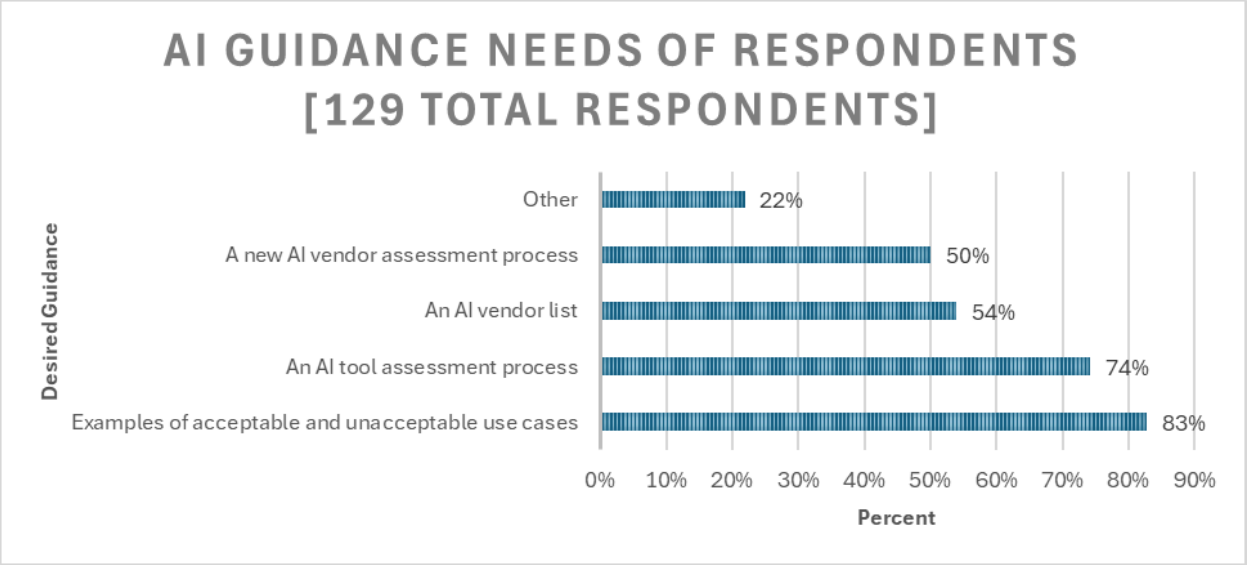


Figure 19

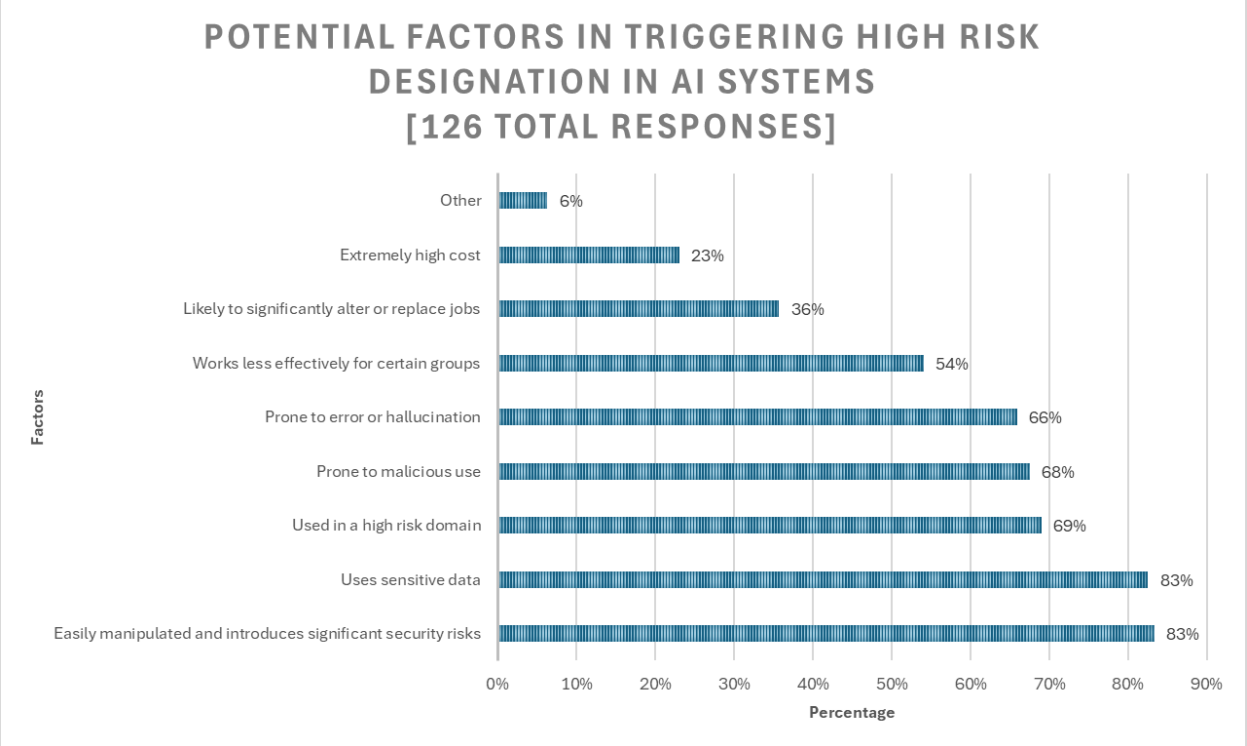


Figure 20

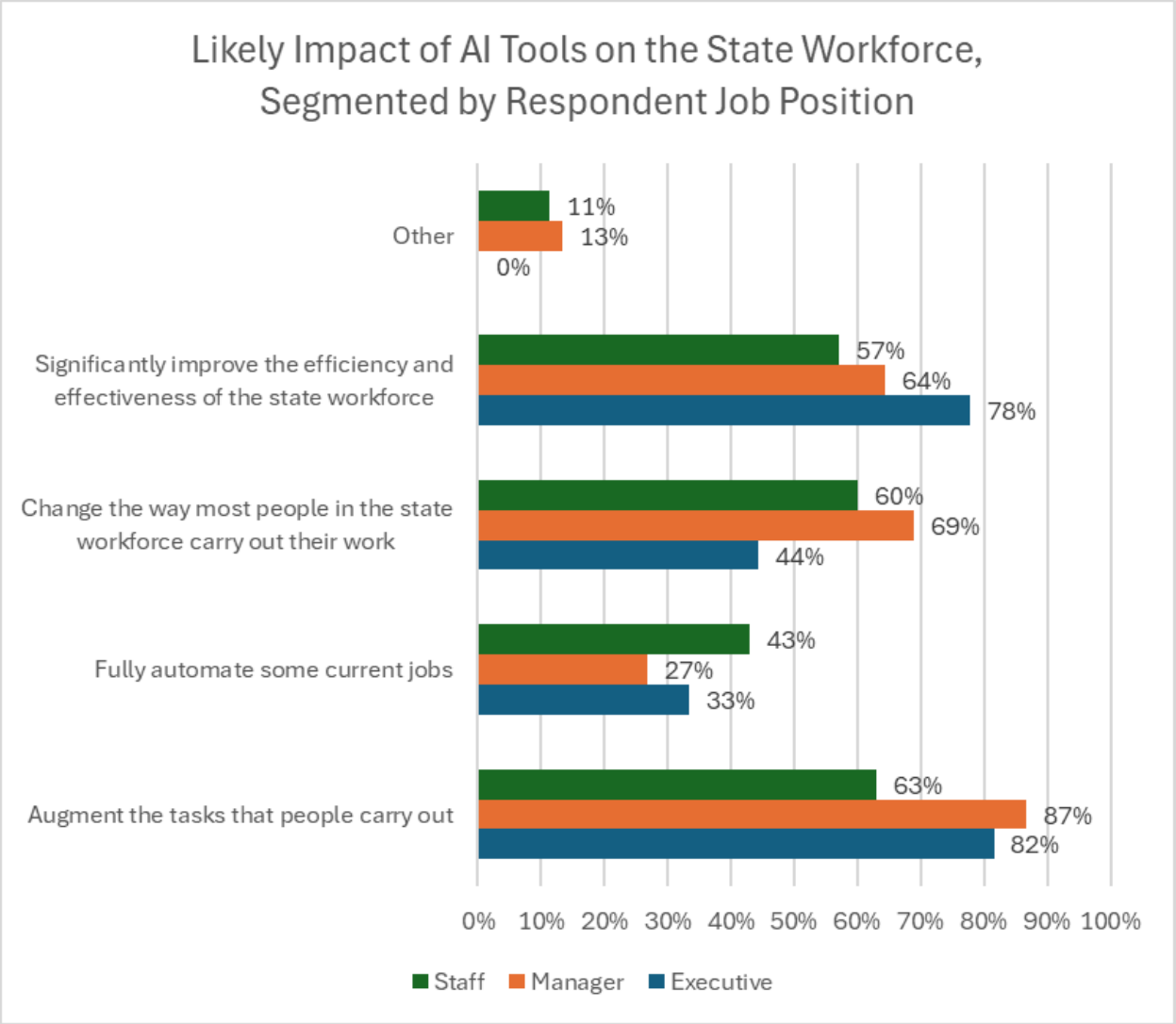

Likely Impact of AI Tools on the State Workforce, Segmented by Respondent Job Position
Other
11%
13%
0%
Significantly improve the efficiency and effectiveness of the state workforce
57%
64%
78%
Change the way most people in the state workforce carry out their work
60%
69%
44%
Fully automate some current jobs
43%
27%
33%
Augment the tasks that people carry out
63%
87%
82%
0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
Staff
Manager
Executive

Figure 21

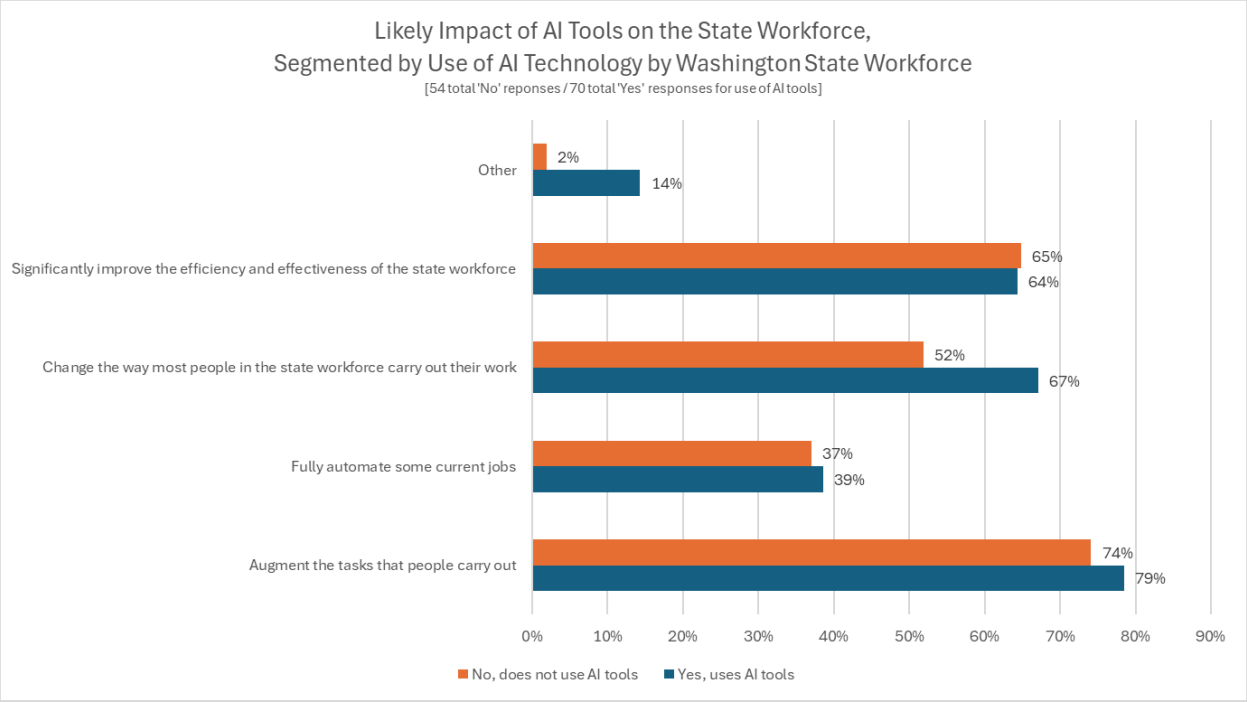


Figure 22

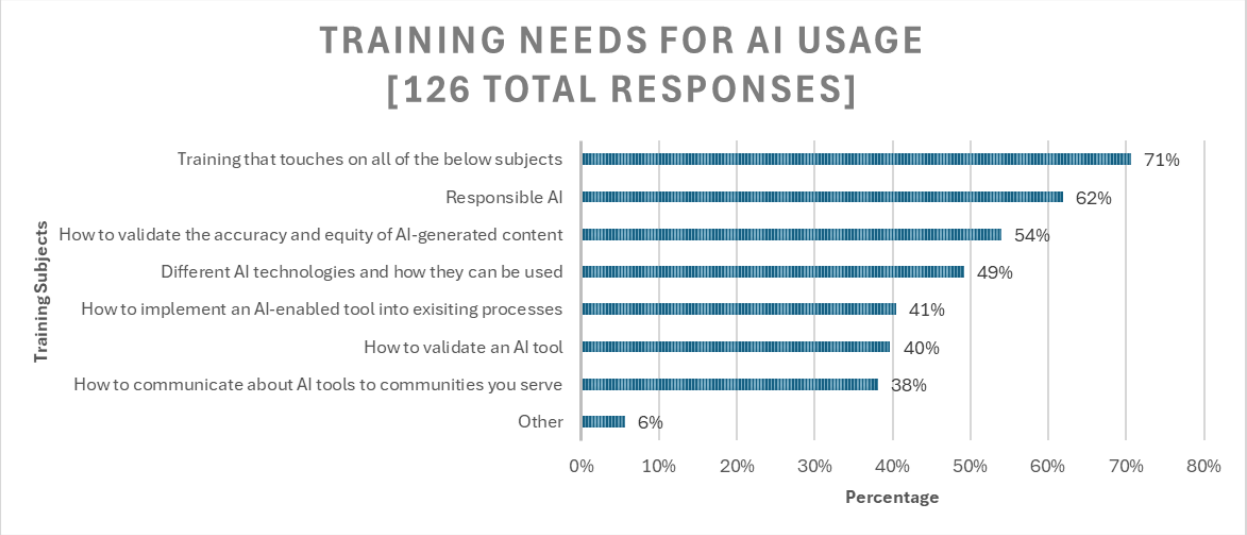
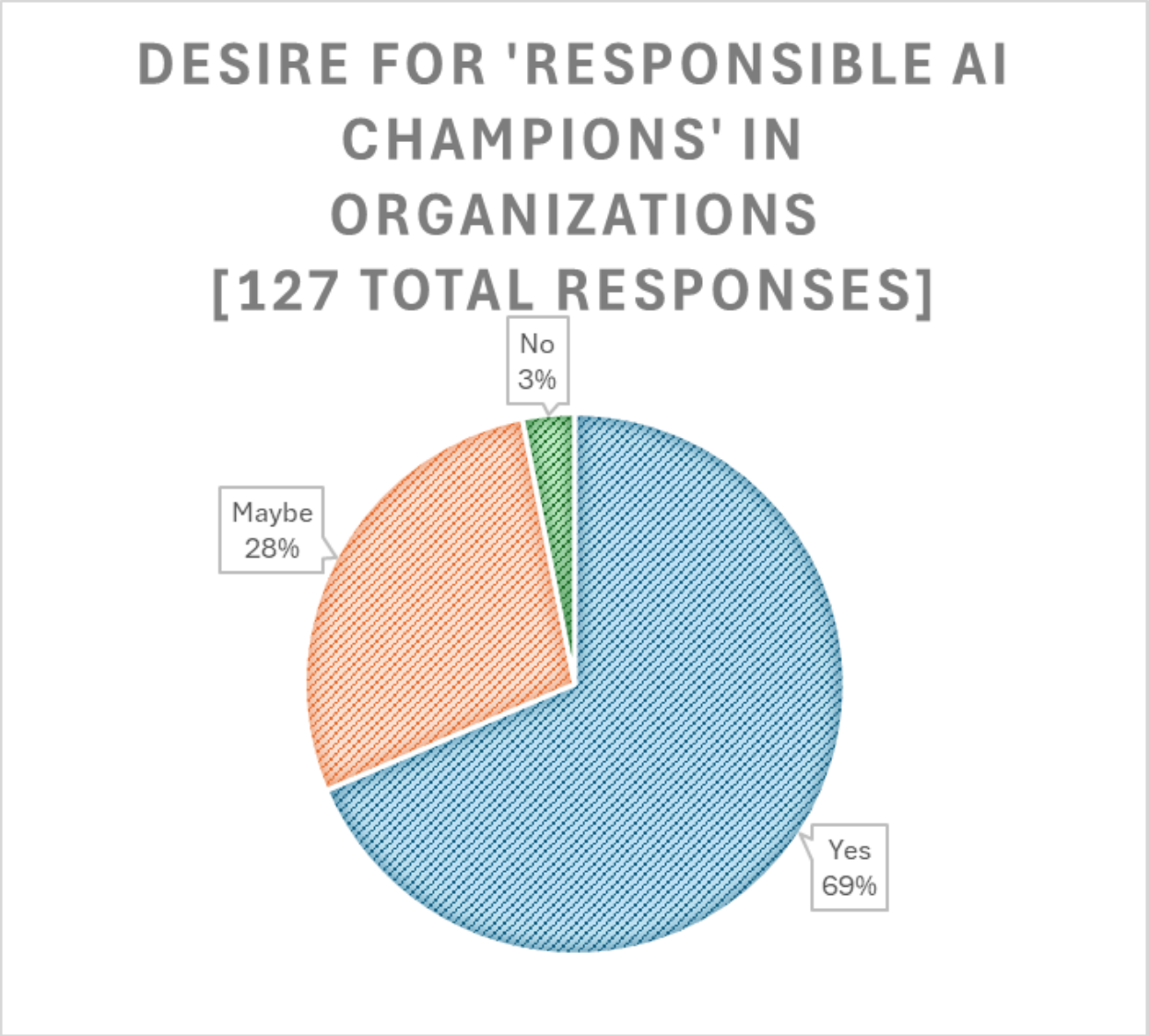


Figure 23


DESIRE FOR 'RESPONSIBLE AI CHAMPIONS' IN ORGANIZATIONS [127 TOTAL RESPONSES]
No 3%
Maybe 28%
Yes 69%

WaTech
Washington Technology Solutions

CITRIS
THE BANATAO INSTITUTE

CITRIS POLICY LAB

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Need help navigating your responsible AI strategy?
Visit CITRISPolicyLab.org or contact Brandie Nonnecke, PhD (nonnecke@berkeley.edu)