APRIL 2024

The Federal Government's Power of the Purse

Enacting Procurement Policies and Practices to Support Responsible AI Use

Hannah Quay-de la Vallee
Ridhi Shetty
Elizabeth Laird

CENTER FOR
DEMOCRACY
& TECHNOLOGY

CENTER FOR
DEMOCRACY
& TECHNOLOGY

The **Center for Democracy & Technology (CDT)** is the leading nonpartisan, nonprofit organization fighting to advance civil rights and civil liberties in the digital age. We shape technology policy, governance, and design with a focus on equity and democratic values. Established in 1994, CDT has been a trusted advocate for digital rights since the earliest days of the internet. The organization is headquartered in Washington, D.C. and has a Europe Office in Brussels, Belgium.

APRIL 2023

The Federal Government's Power of the Purse

Enacting Procurement Policies and Practices to Support Responsible AI Use

Hannah Quay-de la Vallee, Ridhi Shetty, and Elizabeth Laird

This report was created with consulting support from Dave Zvenyach, Independent Consultant.

With contributions from Tim Hoagland on layout and design.

This CDT report is informed by interviews with experts within a variety of organizations representing different perspectives, including the federal government, academia, industry, and civil society organizations.

CENTER FOR
DEMOCRACY
& TECHNOLOGY

ES

Executive Summary

Government spending on artificial intelligence (AI) has reached unprecedented levels. In fiscal year 2022, the United States government awarded over $2 billion in contracts to private companies that provide services that rely on AI, and total spending on AI has increased nearly 2.5 times since 2017.[1]

Meanwhile, federal policymakers’ attention to AI continues to grow, with multiple legislative and executive actions aimed at encouraging the federal government to adopt AI while accounting for issues of bias, privacy, transparency, and efficacy. The increase of government spending on AI, in addition to the growing acknowledgement of the potential and risks associated with such technology, has raised new

[1] Institute for Human-Centered AI, Stanford University, The AI Index 2023 Annual Report (April 2023) https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf#page=288 [https://perma.cc/8REP-SS29].

and urgent questions about whether and how tenets of responsible AI use are addressed in federal government procurement policies and practices.

Building on years of bipartisan federal efforts to govern AI use – including legislation, agency actions and guidance, and executive orders – two recent executive actions have taken direct aim at the federal government's procurement of AI: the Biden Administration's 2023 **Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence** (2023 AI EO)[2] and the Office of Management and Budget's (OMB) subsequent guidance, the 2024 **Memorandum for Agency Use of AI** (Final OMB AI Memo).[3] The Biden Administration's 2023 Executive Order on Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government (2023 Racial Equity EO) also requires that agencies designing, developing, acquiring, and using AI and automated systems must do so in a manner that advances equity.[4]

The 2023 AI EO lays out a whole-of-government strategy for federal agencies to support robust AI governance, including by the public sectors. It specifically addresses procurement by focusing on expansion of the federal workforce to ensure that the government has the ability to appropriately solicit and assess procured AI systems, clarifying expectations of the guidelines procured AI systems are expected to adhere to, and directing OMB to provide guidance to agencies on the design, use, and procurement of AI systems.

Following the 2023 AI EO, OMB released the required agency guidance, the Final OMB AI Memo in March 2024 (following a round of comments on a

[2] Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence [hereinafter "2023 AI EO"] (Oct 30, 2023) https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [https://perma.cc/ZVJ4-8WKP].

[3] Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence [hereinafter "Final OMB AI Memo"] (Mar 28, 2024) 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 [https://perma.cc/3XVW-LGWE].

[4] Executive Order 14091 On Advancing Racial Equity and Support for Underserved Communities Through the Federal Government (Feb 16, 2023), https://www.whitehouse.gov/briefing-room/presidential-actions/2023/02/16/executive-order-on-further-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government/ [https://perma.cc/GTG2-CGVG].

proposed version).[5] The Final OMB AI Memo provides extensive guidance on the use of AI systems and will invariably impact procurement processes because agencies need confidence that a procured system can comply with the Memo's requirements. The Final OMB AI Memo also provides some explicit procurement recommendations, including aligning procured systems to legal requirements, increasing transparency on procured systems, and promoting competition. Both the AI Executive Order and Final OMB AI Memo are important steps to guide AI procurement, but to achieve the goal of equitable, ethical, and effective government procurement of AI more support is needed, including more robust guidance from OMB.

Individual federal agencies are still, nonetheless, making decisions about whether and how to procure AI-driven technology from third parties. In doing so, they face a number of challenges specific to the AI context, particularly for the purpose of service delivery. This report identifies a number of these challenges, including the lack of a common definition of AI, limited internal capacity to evaluate AI-driven systems and the vendors that provide them, and insufficient monitoring contracts for AI systems after they have been executed. Additionally, limitations within existing federal procurement processes threaten to further impede the responsible procurement of AI. These include difficulties around understanding and evaluating bias, incorporating human oversight and intervention, and defining and implementing a process for redress in the event that an AI-driven system results in harm.

This report provides a number of recommendations to establish robust and sustainable AI procurement processes for federal agencies. The report is informed by interviews with current and former government employees, and experts representing different perspectives from academia, industry, and civil society organizations. It recommends that the following federal actions should be taken:

[5] Final OMB AI Memo; Office of Management and Budget, Proposed Memorandum for the Heads of Executive Departments and Agencies on Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence [hereinafter "Proposed OMB AI Memo"] (2023), https://ai.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-Public-Comment.pdf [https://perma.cc/2LNK-T5TD]. The Memo had also been required by the AI in Government Act, Consolidated Appropriations Act, 2021, Pub. L. No. 116–260, div. U, Title I, Sec. 104 https://www.congress.gov/bill/116th-congress/house-bill/133.

- **Incorporate responsible AI considerations at the acquisition planning stage.** This should include encouraging agencies to build upon the processes in the Federal Acquisition Regulations to consider the potential socio-technical risks of AI on end-users or intended beneficiaries; developing an "AI Responsibility Questionnaire" built for government agencies to use as part of procurement planning and market research; and encouraging agencies to require legal review for all contracts that involve AI to ensure equity.

- **Include references to AI risks in the Federal Acquisition Regulations.** The references should explicitly call out and emphasize responsible AI practices in areas such as acquisition planning, market research, privacy protection, and quality assurance.

- **Equip agencies to perform pre-award vendor evaluation and post-award vendor monitoring.** Federal agencies would benefit from guidance on how to make broader use of their authority to conduct pre-award evaluations for AI models; how to further develop standards or certifications for responsible AI similar to efforts like Federal Risk and Authorization Management Program; and support and resources on how to build independent auditing into the acquisition process.

- **Clarify and strengthen transparency, reporting, and oversight requirements and issue guidance to facilitate compliance.** Cross-government bodies such as Congress, OMB, and the GAO should take steps such as providing a consistent definition of AI systems; strengthening the "AI inventories" for greater transparency around agency AI use; advocating for the addition of specific reporting requirements regarding responsible AI in the Federal Information Technology Acquisition Reform Act (FITARA) scorecard; developing guidance and taking a consistent approach to intellectual property provisions in vendor contracts; publishing an "oversight guide" for reviewing agency acquisition activities; strengthening requirements for agencies to conduct Algorithmic Impact Assessments (AIAs) and require agencies to publish them on their websites; and encouraging the National Institute of Standards and Technology (NIST) to adopt a standard for AIAs.

- **Increase federal workforce capacity to ensure agencies are prepared to evaluate and manage risks throughout AI procurement.** Agencies should develop training modules and incorporate them into the existing procurement curriculum, and encourage the growth and support of digital-services teams within the government with experience designing and deploying responsible AI.

While this report focuses on federal AI procurement policy, the federal government can also ensure that federal taxpayer dollars are used responsibly by establishing requirements for and oversight of grants that support state, local, and private sector uses of AI.[6] In addressing federal AI procurement, the following report is intended to provide a framework for how to enable procurers of AI within the federal government to acquire systems that will strengthen and improve agency operations while protecting the people those agencies are made to serve.

[6] CDT has provided recommendations on how policymakers can make the best use of grant-making authorities, including by requiring agencies' chief AI officers to provide resources and oversight to grantmaking processes that touch on AI. Center for Democracy & Technology, *Comment to Office of Management and Budget on Proposed Memorandum on Agency Use of AI* (Dec 5, 2023), https://cdt.org/insights/cdt-comments-on-omb-draft-guidance-for-agency-use-of-ai/ [https://perma.cc/EH5Z-6K8P]; Dan Bateyko, *Taken for Granted: Where's the Oversight of AI and Federal Funding*, Center for Democracy & Technology (Aug 7, 2023), https://cdt.org/insights/taken-for-granted-wheres-the-oversight-of-ai-and-federal-funding [https://perma.cc/7CZA-36RN].

Contents

02 A Brief History of Federal AI Procurement Governance

Bipartisan coalitions in Congress and both the Trump and Biden Administrations have aimed to address the federal government's use of AI, trying to promote the development and adoption of AI while also advancing standards and processes for AI accountability and good governance. Recent years have seen numerous actions that will shape the federal government's procurement or AI going forward, both by direct procurement guidance and by regulations on the government's *use* of AI, which in turn implicate how it *procures* AI. This range of actions has also created a complex landscape of regulations, guidance, and definitions of AI. (Appendix A offers a more detailed, though not exhaustive, timeline of federal government actions on the use and procurement of AI systems).

Legislative approaches have impacted procurement directly and indirectly. Directly, the **Advancing American AI Act**[7] and

[7] *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, Pub. L. No. 117-263 https://www.congress.gov/bill/117th-congress/house-bill/7776.

the **Training for the Acquisitions Workforce Act** (AI Training Act)[8] both pushed for further input on procurement from OMB and the Government Services Administration (GSA) (as well as development of an AI-ready federal government workforce). Indirectly, several acts have implicated procurement by governing other aspects of government AI use (impacting how procured systems must operate): The **John S. McCain National Defense Authorization Act for Fiscal Year 2019** (McCain NDAA) included the first legislative definition of AI, while the **National Artificial Intelligence Initiative Act of 2020**[9] served primarily to coordinate AI research and development activities across federal agencies, and the **AI in Government Act of 2020**[10] encouraged the adoption of AI by federal agencies.

In addition to federal agencies outlining their own strategies on their use of AI,[11] other actors have established frameworks and guidance that can inform agencies' AI use and procurement. In January 2023, the National Institute of Standards and Technology (NIST) published the **AI Risk Management Framework 1.0** (AI RMF),[12] which, like much of the AI legislation, can impact procurement by providing guidance on the use and design of

[8] *AI Training Act*, Pub. L. No. 117-207 https://www.congress.gov/bill/117th-congress/senate-bill/2551.

[9] *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, Pub. L. No. 116–283 https://www.congress.gov/bill/116th-congress/house-bill/6395.

[10] *Consolidated Appropriations Act, 2021*, Pub. L. No. 116–260 https://www.congress.gov/bill/116th-congress/house-bill/133.

[11] Department of Defense, *Implementing Responsible Artificial Intelligence in the Department of Defense* (May 26, 2021) https://media.defense.gov/2021/May/27/2002730593/-1/-1/0/implementing-responsible-artificial-intelligence-in-the-department-of-defense.pdf [https://perma.cc/BBH4-6YN4]; Department of Homeland Security, *Establishment of a DHS Artificial Intelligence Task Force* (April 20, 2023) https://www.dhs.gov/sites/default/files/2023-04/23_0420_sec_signed_ai_task_force_memo_508.pdf [https://perma.cc/7V2T-L4R8]; Department of Health and Human Services, *Artificial Intelligence (AI) Strategy* (Jan 2021) https://www.hhs.gov/sites/default/files/final-hhs-ai-strategy.pdf [https://perma.cc/Z6UM-XN7Z]; Department of Veterans Affairs, *Artificial Intelligence (AI) Strategy* (July 2021) https://www.research.va.gov/naii/VA_AI_Strategy_V2-508.pdf [https://perma.cc/G2L4-5YWE].

[12] National Institute of Standards and Technology, *AI Risk Management Framework,* (Jan 26, 2023) https://www.nist.gov/itl/ai-risk-management-framework [https://perma.cc/3QVN-9WCF].

AI systems, thus impacting how agencies will need to evaluate systems during procurement (and after deployment). Similarly, the Administrative Conference of the United States (ACUS) has issued cross-governmental guidance and recommendations regarding the administrative law and practice issues raised by federal agencies' use of AI,[13] which applies to procured systems as well as those developed internally. The GAO also published a 2021 Framework for key accountability practices to help federal agencies and others use AI responsibly, emphasizing principles of governance, data, performance, and monitoring.[14]

Executive actions across administrations have also provided guidance relevant to the AI procurement process, whether directly or by governing AI use. From the Trump Administration, **Executive Order 13859 on Maintaining American Leadership in Artificial Intelligence** focused on ensuring United States leadership in "AI R&D and deployment" while **Executive Order 13960 on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government** (Executive Order 13960)[15] set forth a policy "to promote the innovation and use of AI" to improve government services while still fostering public trust and confidence and remaining "consistent with all applicable laws, including those related to privacy, civil rights, and civil liberties."

Building on the previous administration's actions, the Biden Administration has issued several elements of guidance for AI.

[13] Administrative Conference of the United States, *Agency Use of Artificial Intelligence* (Dec 31, 2020) https://www.acus.gov/recommendation/agency-use-artificial-intelligence [https://perma.cc/ZE5H-PGYS]; Administrative Conference of the United States, *Recommendation 2022-3, Automated Legal Guidance at Federal Agencies* (June 28, 2022) https://www.acus.gov/recommendation/automated-legal-guidance-federal-agencies [https://perma.cc/KZK3-6YL9].

[14] Government Accountability Office, *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities*, [hereinafter "GAO AI Accountability Framework"] (June 30, 2021), https://www.gao.gov/products/gao-21-519sp [https://perma.cc/67EX-A3K3].

[15] Executive Order 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government* (Dec 2020) https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government [https://perma.cc/P5SD-NWFZ].

Executive Order 14091 on Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government (2023 Racial Equity EO)[16] explicitly addresses procured systems, mandating that "[w]hen designing, developing, acquiring, and using artificial intelligence and automated systems" the government must stay "consistent with applicable law, in a manner that advances equity."[17] The **Blueprint for an AI Bill of Rights** (Blueprint), published by the Office of Science and Technology Policy in October 2022, established "principles and associated practices to help guide the design, use, and deployment of automated systems to protect the rights of the American public in the age of artificial intelligence."[18] Notably, the Blueprint contains an extensive appendix that details examples of harms arising from poorly designed or unaccountable AI systems, and positive interventions that can mitigate those harms, which can help procurers evaluate vendor offerings and ensure they are used safely.

[16] 2023 Racial Equity EO.

[17] *Id.* at Sec. 4(b).

[18] White House Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights* (2022), https://www.whitehouse.gov/ostp/ai-bill-of-rights/ [https://perma.cc/BAH3-3M5T].

03 Current Federal AI Procurement Priorities

On October 30, 2023, President Biden signed **Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence** (2023 AI EO)[19] which (among many other provisions) elaborates on federal agencies' obligations in the use and acquisition of AI.[20] It directs OMB to require each agency to designate a Chief AI Officer (CAIO) who is responsible for governing that agency's use and procurement of AI (including ensuring that acquisitions implement the principles identified in Executive Order 13960 and the 2023 Racial Equity EO). It also lays out government-wide requirements, including directing OMB to issue guidance on agencies' use of AI and management of AI risks. The Order directs NIST to "develop guidelines, tools, and practices to support implementation of the minimum risk-management practices" set forth in OMB's guidance, and directs OMB to "develop an initial means to ensure that agency contracts for the acquisition of AI systems and services align with" its guidance.[21]

Following the AI EO, OMB issued the **Proposed Memorandum for Agency Use of AI** (Proposed OMB AI Memo)[22] on November 3, 2023, which had also been mandated by the AI in Government Act of 2020. Following a public comment period from November 3 to

[19] 2023 AI EO.
[20] *Id.* at Sec. 10(b)(i).
[21] *Id.* at Sec. 10.1(d).
[22] Proposed OMB AI Memo.

December 5, 2023, OMB released the final version March 28, 2024 (Final OMB AI Memo).[23] CDT and a number of other organizations filed comments to the Proposed OMB AI Memo, including how to improve its guidance on AI procurement.[24]

The Final OMB AI Memo aims to strengthen governance of AI in the federal government both within and across agencies. The Memo sets out measures for increased coordination within and between agencies; steps for advancing responsible AI innovation; and criteria for agencies to identify and manage risks from the use of AI, including minimum risk management practices for AI uses that are likely to impact "rights and safety." It also contains important transparency provisions for agencies to disclose their rights- and safety-impacting AI uses, building on earlier transparency requirements in Executive Order 13960.

Because these frameworks will apply to federal government uses of AI whether the system is built in-house or procured, the Final OMB AI Memo also offers recommendations on the procurement of AI systems. It suggests that each agency's CAIO and AI governance board should coordinate with agency procurement officials to manage AI risks.[25] Further, the Final OMB AI Memo recommends that agencies:

- Ensure that their procured AI aligns with constitutional, civil rights, and all other applicable laws, regulations, and policies;
- Ensure transparency and adequate performance of their procured AI, including through adequate documentation of known limitations and data used to train AI, regular evaluation of vendors' effectiveness claims and risk management processes, contractual provisions incentivizing continuous improvement, and appropriate post-award monitoring;
- Take appropriate steps to promote competition between contractors;

[23] Final OMB AI Memo.

[24] Ridhi Shetty and Alexandra Reeve Givens, *Civil Rights Organizations Identify Priorities for OMB Memo on Agency Use of AI*, Center for Democracy & Technology (Jan 26, 2024) https://cdt.org/insights/civil-rights-organizations-identify-priorities-for-omb-memo-on-agency-use-of-ai/ [https://perma.cc/ZX7C-C4JD].

[25] Final OMB AI Memo, Sec. 3(b)(ii)(U) and 3(c)(ii).

- Contractually retain rights to data used by their procured AI so that they can manage the development, testing, and use of the AI and protect the data from unauthorized use and disclosure as well as avoid vendor lock-in;
- Avoid testing vendor systems on the same data they were trained on, which could result in a system that seems accurate during testing but would not perform well in real-world deployment; and
- Include specific risk management requirements tailored to procurement of AI for biometric identification or generative AI dual-use foundation models in their contracts.[26]

These recommendations highlight key challenges in procurement and create an important baseline for what responsible procurement guidance must address. However, the recommendations are high-level, and fall far short from the detailed, actionable guidance that agencies – and individual procurement officers – will need to navigate AI procurement with effectiveness and consistency. For these reasons, more instructive guidance is needed, both in the form of more fulsome and detailed OMB guidance, along with clarified and updated transparency requirements and acquisition regulations for an AI context, and a government workforce with the skills and knowledge to effectively assess and deploy AI systems.

[26] *Id.* at Sec. 5(d)(v).

04

Unique Risks and Governance Challenges of AI Procurement

Historically, the federal government (in addition to state and local agencies) has struggled to effectively build and buy software. As such, many challenges that exist with AI procurement (e.g., business models, novelty of the technology, limited workforce capacity, intellectual property issues, etc.) are not specific to AI. Nevertheless, AI presents unique risks that should be addressed during the acquisition process.

NIST's AI Risk Management Framework offers a helpful starting point from which to identify unique procurement challenges presented by AI. For instance, as NIST recognizes, datasets used to train AI systems may become detached from their original and intended context or may become stale or outdated relative to the deployment context. This is a particular challenge because procurements are often structured toward the creation of long-term contracts (typically, 5 years). Re-training AI will need to be built into procurements. If agencies procure systems from other agencies, this may add to the risk of systems becoming detached from their intended contexts. An extensive list detailing particular AI risks and how they can impact the procurement process is provided in Appendix B.

In addition to the AI-specific risks described in the AI RMF, the novelty and complexity of AI procurement in government, along with its lack of technical capacity, raises additional concerns:

A. The federal government lacks a common definition of AI.

Despite years of efforts to govern AI, there is no agreement on what "AI" means, with various pieces of legislation and guidance providing different definitions.

For example, the National Artificial Intelligence Initiative Act defines AI to mean "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments" while the AI in Government Act relied on the McCain NDAA's five-part definition of AI, which has now been adopted in the Final OMB AI Memo.[27] There can even be variation within a given document; the 2023 AI EO relies on the National Artificial Intelligence Initiative Act's definition generally, but requires agencies' Chief AI Officers to coordinate implementation of the principles set forth in the Trump-era Executive Order 13960, which uses the McCain NDAA definition.

[27] The McCain NDAA defines AI as: "(1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets. (2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action. (3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks. (4) A set of techniques, including machine learning, that is designed to approximate a cognitive task. (5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting."

These definitions also take a range of approaches: In some cases AI is defined primarily by its use to arrive at particular *outcomes* (i.e., making a prediction, recommendation, or decision, per the National Artificial Intelligence Initiative Act approach), in others by its *mechanism* (i.e., supervised and unsupervised learning, per the McCain NDAA).[28]

These disparate definitions reflect uncertainty about which systems count as AI, and consequently what governance and rules structures should apply to a given system. For example, the NASA Inspector General's office noted that having multiple definitions of AI leads to internal monitoring and reporting challenges, writing: "Personnel we interviewed stated they reported AI based on their own individual understanding of what the term means rather than a formal definition provided by the Agency. As a result, NASA does not have a singular designation or classification mechanism to accurately classify and track AI... making it difficult for the Agency to meet federal requirements to monitor its use of AI."[29]

[28] Compounding the problem, Executive Order 13960 narrowed the definition by excluding from its scope any "AI embedded within common commercial products, such as word processors or map navigation systems" and any "AI research and development (R&D) activities." These exclusions, in practice, exclude a broad swath because the term "commercial product" has a specific legal meaning laid out in 41 USC § 103 that excludes a significant portion of what non-practitioners might assume constitutes the use of AI by the federal government.

[29] NASA Office of Inspector General, *NASA's Management of Its Artificial Intelligence Capabilities* (May 3, 2023) https://oig.nasa.gov/wp-content/uploads/2023/12/ig-23-012.pdf [https://perma.cc/V4X7-UUSU].

B. Individual federal agencies lack capacity to properly evaluate vendors and rely on vendors, including bias identification and mitigation.

Although the federal government continues to increase the amount of money obligated on contracts every year, the acquisition workforce is not growing to meet the demand. The decline in acquisition capacity has created significant risks in the federal government. Indeed, the Government Accountability Office's (GAO) High-Risk List includes at least six areas where acquisition management is identified as high-risk.[30]

This limited capacity is further challenged by the novelty and complexity of effectively managing AI. Ultimately, there are not enough individuals in government with the time or expertise to oversee AI vendors.[31] Consequently, the government heavily relies on the vendors themselves to determine how AI products should be evaluated for quality and performance and to carry out those evaluations. This issue is exacerbated by the fact that, in some cases, it is considered a best practice for performance-based acquisition to have the contractor be responsible for proposing

[30] Government Accountability Office, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, GAO-23-106203 (April 20, 2023) https://www.gao.gov/products/gao-23-106203 [https://perma.cc/R9H2-YFCF].

[31] Ross Wilkers, *Acquisition Shops Inside Government Need Workers Too*, Washington Technology (June 24, 2022), https://washingtontechnology.com/contracts/2022/06/acquisition-shops-inside-government-need-workers-too/368569/ [https://perma.cc/LRT5-EMW3].

performance metrics.[32]

Agencies’ reliance on vendors is concerning because vendors can make claims about what AI can accomplish without offering sufficient evidence, raising concerns about whether AI actually *works* for government use cases.[33] The inability to assess systems is often accompanied by pressure to adopt AI as an innovation measure, not just as a means to more effective service delivery.[34] This framing encourages greater risk taking and subtly shifts the expectations away from government management of the process – is it indeed making an agency’s service delivery more effective? – to a greater deference to and dependency on proprietary methods. Rhetoric around innovation and great-power competition can create an environment where the government is less skeptical of AI than it should be, worsened by lack of visibility into what the AI system is actually capable of doing.

Agencies’ lack of visibility and effective evaluation capacity presents significant concerns related to identifying and mitigating bias and inequity in AI systems. Although these concerns are present in many non-AI systems used by the government, AI models introduce unique risks of bias and inequity affecting the individuals and communities subject to these systems.[35]

[32] *See* General Services Administration, *Steps to Performance-Based Acquisition, Step 5*, “Contractor Proposed the Metrics and QAP” (accessed Mar 29, 2024). (“One widely used approach is to require the contractor to propose performance metrics and the Quality Assurance Plan (QAP), rather than have the government develop it. This is especially suitable when using a Statement of Objectives (SOO) because the solution is not known until proposed. With a SOO, offerors are free to develop their own solutions, so it makes sense for them to develop and propose a QAP that is tailored to their solution and commercial practices. If the agency were to develop the QAP, it could very well limit what contractors can propose.”) https://buy.gsa.gov/spba/steps?step=acquisition-strategy [https://perma.cc/JS4G-QG9T].

[33] Arvind Narayanan and Sayash Kapoor, *Introducing the AI Snake Oil Book Project* (2022) https://www.aisnakeoil.com/p/introducing-the-ai-snake-oil-book [https://perma.cc/3MMB-T2XQ].

[34] GSA AI Center of Excellence, AI Guide for Government (2024) https://coe.gsa.gov/coe/ai-guide-for-government/introduction/index.html [https://perma.cc/9CZE-YTK9].

[35] *See e.g.,* Grant Fergusson, Electronic Privacy Information Center, *Outsourced and Automated: How AI Companies Have Taken Over Government Decision-Making* 17-21 [hereinafter “Outsourced and Automated”] (2023) https://epic.org/wp-content/uploads/2023/09/FINAL-EPIC-Outsourced-Automated-Report-Appendix-Included.pdf [https://perma.cc/KY7U-K9BY].

NIST Special Publication 1270, Towards a Standard for Identifying and Managing Bias in Artificial Intelligence, identified three categories of challenges in addressing AI bias: issues in the datasets used by the AI, challenges around measurement for testing and evaluation of systems, and human factors like societal biases exhibited by humans interacting with the system.[36]

Unfortunately, government employees may not be aware of the risks of bias during the procurement process. Worse, government employees may be disincentivized from examining the risks of AI bias in specific cases. For example, the GAO noted that government employees may avoid explicitly considering AI bias:

> *One forum participant stated that entities will need to determine whether the model needs adjustment to reduce bias or to address a disparate impact. Without this information, participants stated that entities cannot know how or if the model is performing differently for different demographic groups. According to a participant, some entities are discouraged from collecting protected class data or taking steps to mitigate bias, because doing so may raise risks associated with anti-discrimination liability. Instead, these entities prefer to remain unaware because they consider this the safest way of proceeding.*[37]

Without clear guidance, government employees might avoid classifying projects as "AI" because it forces an analysis of bias that they are unprepared to handle.

[36] National Institute of Standards and Technology, *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence* (2022) https://www.nist.gov/publications/towards-standard-identifying-and-managing-bias-artificial-intelligence [https://perma.cc/JF5D-BQQT].

[37] GAO AI Accountability Framework, *supra* note 14.

C. Individual agencies lack necessary resources to ensure appropriate human oversight and intervention.

Another specific risk introduced by the use of AI is that automation is often considered to be a cost-saving measure, with lower need for human intervention. Although automation may change how humans make decisions, it is important to recognize that monitoring AI and addressing AI's limitations will merely shift the need for human intervention – human engagement and resourcing is still required. When incorporating AI systems into decision-making, agencies will have to ensure that humans ultimately remain responsible for making the relevant decision (in many instances this is not just a best practice, but a legal requirement if the agency action impacts people's rights).[38] Their workforce will also need to be trained on the systems' limitations, how to mitigate automation bias, and how to suitably employ human alternatives when a system fails or requires a human to complete the processes for which these systems are used.

To give two examples, if an AI system interferes with service completion, the agency will need to ensure that the beneficiary still has a non-automated (i.e. human) method of completing the workflow, and can access this human alternative in a timely and fair way. Similarly, if facial recognition technology for identity verification fails to positively verify an individual, the provider would need to staff a contact center to allow the individual to complete the identity verification process.

[38] *See, e.g.*, Center for Democracy & Technology, *Challenging the Use of Algorithm-driven Decision-making in Benefits Determinations Affecting People with Disabilities* (Oct 21, 2020) describing due process obligations that govern agencies' use of AI in public benefits determinations https://cdt.org/insights/report-challenging-the-use-of-algorithm-driven-decision-making-in-benefits-determinations-affecting-people-with-disabilities/ [https://perma.cc/3MDH-4DYG].

Because the government lacks sufficient experience managing vendors using AI, it will be important to ensure that agencies build in additional budgets for oversight and staffing associated with those systems. This need for continuous post-award oversight and human intervention is complicated by the conventional approach to federal IT budgeting, which typically contemplates large capital expenditures followed by lower steady-state spending expectations.[39]

D. Cross-government policymaking and resourcing bodies lack necessary expertise, and struggle to provide sufficient detail to support individual agencies.

In addition to individual federal agencies lacking capacity on AI, bodies such as Congress, OMB, GSA, and NIST face some particular challenges in governing or guiding the responsible procurement of AI. Centralized policymaking and technical assistance could theoretically enable better outcomes, but these cross-government bodies themselves require significant staffing changes to provide sufficient expertise. Furthermore, they face a challenging task when issuing guidance or rules that apply to the vast range of federal agencies. Even lengthy documents like the NIST AI RMF or the OMB AI Memo still operate at a certain level of abstraction in order to cover the wide scope of AI uses across the

[39] For a robust discussion about federal budgeting practices and software delivery challenges, *see* Waldo Jaquith et al, *De-Risking Guide*, 18F (accessed April 12, 2024) https://guides.18f.gov/derisking/federal-field-guide/planning/#invest-in-technology-incrementally-and-budget-for-risk-mitigation-prototyping [https://perma.cc/SAA2-FLZ5].

federal government. They must be bolstered by context-specific interpretation, and thus still leave considerable work to individual agencies.

E. Procurement processes do not typically accommodate the continuous monitoring and post-award management required for responsible AI.

Although post-award management is a critical part of the acquisition process, most government contracts emphasize pre-award actions and contract formation rather than the continuous post-award monitoring, evaluation, and model refinement required for responsible AI.

However, the risks associated with responsible AI practices are critical to monitor and address throughout post-award activities. Both NIST and GAO have warned about the need for meaningful post-award monitoring because "AI systems may require more frequent maintenance and triggers for conducting corrective maintenance due to data, model, or concept drift."[40]

Unlike for non-AI acquisitions, agencies that use AI will need to prepare and add new methods for supporting the entire lifecycle of procurement, including, for example, providing input into impact assessments; allowing for transparency and explainability in AI outputs; budgeting for appropriate oversight and remediation with regard to improvement, drift, and bias; and ensuring continuous oversight of vendors' claims of accuracy and performance.

[40] AI RMF, Appendix B, *supra* note 12.

Traditional post-award monitoring is limited to reporting in the Contractor Performance Assessment Reporting System (CPARS), which details how contractors perform with respect to "quality, schedule, cost control, management, and regulatory compliance."[41] There is very little guidance about how agencies should manage vendors post-award other than evaluating a contractor's adherence to a contract.

While the GSA AI Centers of Excellence (GSA CoE) has developed a guide that describes the types of considerations for deploying AI responsibly in production, it is only impactful if agencies are meaningfully planning for post-award monitoring of AI.[42]

The lack of clear roles and responsibilities, and effective post-award monitoring and governance presents unique risks for AI. Agencies should be considering post-award implementation during the acquisition process, and the failure to do so creates the potential for future cost and harm.

[41] Contractor Performance Assessment Reporting System (accessed Mar 21, 2024), https://www.cpars.gov/ [https://perma.cc/T56X-TH8W].

[42] General Services Administration IT Modernization Centers of Excellence, *COE Guide to AI Ethics* (accessed Mar 29, 2024), https://coe.gsa.gov/docs/CoE%20Guide%20to%20AI%20Ethics.pdf [https://perma.cc/Q7FE-WG37].

F. AI raises particular difficulties for individual agencies in identifying and addressing contractor performance issues.

In theory, government contracts are flexible in the ability to hold vendors accountable because contracts generally reserve the right for the government to unilaterally exercise options to extend. This means that the government can walk away from an underperforming vendor by simply not extending the contract.

But government contracts are *practically inflexible* because ending a contract early comes with political and litigation risk and can lead to potential service interruptions if the related AI system has already been rolled out. Accordingly, to ensure accountability, the government usually requires unambiguous performance requirements and multiple rounds of cure notices before the government will end a contract for nonperformance.[43]

Because an AI system's performance will likely be unpredictable until it is used in production, there is a risk that the government — without strong performance expectations and monitoring built into the contract — will tolerate underperformance rather than cancel the contract. Here, too, procurement officers will need to consider new contract measures to create sufficient latitude for ongoing evaluation and assessment.

[43] "The federal government terminates contracts for convenience, default, and cause. Terminations for convenience are used to end contracts without assigning blame to the contractor, though in many cases officials use this type of termination to avoid lawsuits (Cibinic, 2006). Terminations for default and cause are used to end poorly performing contracts for commercial and non-commercial goods and services, respectively." Benjamin M. Brunjes, *A Rendezvous with Discretion: An Analysis of Federal Simplified Acquisition Procedure Contracts* (April 13, 2020) https://dair.nps.edu/bitstream/123456789/4203/1/SYM-AM-20-054.pdf [https://perma.cc/6Z9Y-666W].

G. Vendors and federal agencies are unclear about redress process responsibilities.

Because automated systems alter decision-making processes, agencies need to build in redress processes and otherwise take steps to ensure due process. There are no consistent practices, however, about which party bears the risks and obligations for redressability. This creates a risk for federal agencies and vendors to be misaligned about which party has the obligation to develop or execute redress processes or remediate harm. This means that harms from AI systems may go unaddressed or addressed slowly or ineffectively, leaving the harmed party at loose ends while agencies and vendors establish responsibility. Additionally, the lack of common language in contracts make it difficult for individual agencies to address this issue on their own.

05 Recommendations

A number of improvements to federal policies and practices will promote better outcomes in the federal government's procurement of responsible AI.

One key step to achieve this is for OMB to provide additional detailed guidance to agencies about procurement that goes beyond its Final Memo,[44] as well as for other cross-government resources (GSA, GAO and others) to provide technical assistance and practice guides. The National Artificial Intelligence Advisory Committee has echoed this call, urging agencies to adopt formal strategies that, among other things, (1) "[p]romote responsible AI innovation, where appropriate, within the agency through deliberative design, development, and deployment"; (2) "[t]est AI applications in a manner that ensures compliance with law and public values"; and (3) "[r]equire substantiation of vendor claims about AI."[45] OMB has begun the process of providing such guidance: the Final OMB AI Memo affirms that procured AI should be rights-respecting; emphasizes the importance of transparency and testing, especially for procurement of biometric identification and generative AI

[44] *Civil Rights Organizations Identify Priorities for OMB Memo on Agency Use of AI, supra* note 24.

[45] National Artificial Intelligence Advisory Committee, *Year 1 Report* (May 2023) https://www.ai.gov/wp-content/uploads/2023/05/NAIAC-Report-Year1.pdf [https://perma.cc/N66Z-WPED].

systems; and calls on agencies to promote vendor competition and oversee how vendors train their AI systems.[46] To build on these recommendations, OMB has solicited public input on guidance specifically for agency procurement of AI.[47]

In essence, the government should be encouraged to be *deliberate* and appropriately *skeptical* of AI during the procurement process, and to require rights-respecting, responsible government use of AI "without unduly stifling innovation."[48] Detailed OMB guidance on AI procurement and other developments to improve federal practices should build on existing processes and practices throughout the acquisition lifecycle that can — and should — be used to achieve better outcomes.

A. Incorporate responsible AI considerations at the acquisition planning stage.

The Federal Acquisition Regulations (FAR) generally requires that agencies conduct acquisition planning to "ensure that the Government meets its needs in the most effective, economical, and timely manner."[49] Additionally, the FAR specifies numerous

[46] Final OMB AI Memo, Sec. 5(d)(vi)-(vii).

[47] Office of Management and Budget, *Request for Information: Responsible Procurement of Artificial Intelligence in Government*, 89 Fed. Reg. 22196 (Mar 29, 2024) https://www.federalregister.gov/documents/2024/03/29/2024-06547/request-for-information-responsible-procurement-of-artificial-intelligence-in-government [https://perma.cc/J6QN-F98V].

[48] *Id*; Center for American Progress, *Comments to OMB on Proposed Memorandum on Agency Use of AI* (2023), https://www.americanprogress.org/wp-content/uploads/sites/2/2023/12/CAP-Draft-OMB-Comments-Final-12.04.2023.pdf [https://perma.cc/8HNC-APNP].

[49] *Federal Acquisition Regulation* [hereinafter "FAR"], *Part 7.102* (accessed April 11, 2024) https://www.acquisition.gov/far/part-7#FAR_7_102__d415e69 [https://perma.cc/5HBV-4MCC].

considerations that written acquisition plans must address,[50] and many considerations for responsible AI should also be documented as part of the acquisition planning process.

Because the acquisition-planning process is already required and well-understood by the acquisition community, and because it allows for meaningful involvement of policymakers before specific vendors or solutions are identified, the acquisition planning stage should be leveraged to include responsible AI considerations.

This could be achieved through several means. Although the FAR includes specific requirements for acquisition plans, agencies have discretion to go beyond the FAR requirements. As such, changes to acquisition planning can come through formal amendments to the FAR, central guidance from OMB, or by individual agencies (who may choose to expand existing processes such as Authority to Operate frameworks to incorporate AI-specific risks).

Specifically, the following interventions should be considered by individual federal agencies during acquisition planning:

- **Emphasize that acquisition planning should explicitly consider the potential socio-technical risks of AI on end-users or intended beneficiaries.** The FAR requires written acquisition plans to document "technical, cost, and schedule risks and describe what efforts are planned or underway to reduce risk and the consequences of failure to achieve goals."[51] Meanwhile, NIST's AI Risk Management Framework explains that "[c]ore concepts in responsible AI emphasize human centricity, social responsibility, and sustainability. AI risk management can drive responsible uses and practices by prompting organizations and their internal teams who design, develop, and deploy AI to think more critically about context and potential or unexpected negative and positive impacts."

[50] FAR, *Part 7.105* https://www.acquisition.gov/far/part-7#FAR_7_105 [https://perma.cc/6WQU-6DBB].

[51] *Id.*

Agencies should explicitly consider the *socio-technical* aspects of AI and outline how they will manage AI risks—including the very real risks that an AI tool simply will not work or will perpetuate or exacerbate bias—as part of acquisition planning.[52]

- **Develop (or facilitate the development of) a standalone "AI Responsibility Questionnaire" built for government agencies to use as part of procurement planning and market research.** When conducting market research as part of acquisition planning, agencies often use Requests for Information (RFIs) to determine whether companies are able to meet government requirements. A well-structured RFI or questionnaire can help the government meaningfully evaluate the competitive landscape[53] and can signal the government's goals to vendors and industry.[54]

  An AI Responsibility Questionnaire[55] could help formalize some of the considerations that agencies should take into account, and could be developed in modular fashion to suit different agencies' fact patterns and contexts. A questionnaire can also establish expectations for industry about the types of questions that

[52] Not only are non-automated alternatives critical to minimize negative impacts on affected members of the public, but having these alternatives in place can minimize litigation costs for agencies. *Outsourced and Automated, supra* note 35, at 61-62.

[53] Results for America, *An RFI Guide: How Requests for Information Can Improve Government Human Services Contracting* (2019) https://results4america.org/rfi-guide/ [https://perma.cc/MGX2-Z3FM].

[54] David Rubenstein, *Acquiring Ethical AI*, 73 Florida L. Rev. 747, 806 (2021) ("More generally...centering ethical AI in market solicitations will signal to prospective vendors that they will need to compete on the field of ethical AI to win federal contracts.") https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3731106 [https://perma.cc/DE8S-D4VY].

[55] *See, e.g.*, Ford Foundation, *A Guiding Framework for Vetting Technology Vendors Operating in the Public Sector* (2023) https://www.fordfoundation.org/wp-content/uploads/2023/03/final_ford-foundation-guiding-framework-r3-full-document-final2.pdf [https://perma.cc/4JYV-3RVH]; GSA AI COE, *Guide to AI Ethics, supra* note 42; Hannah Quay-de la Vallee and Natasha Duarte, *Algorithmic Systems in Education: Incorporating Equity and Fairness When Using Student Data* at 27-28, Center for Democracy & Technology (Aug 12, 2019) https://cdt.org/insights/algorithmic-systems-in-education-incorporating-equity-and-fairness-when-using-student-data/ [https://perma.cc/JQH3-P5L8].

companies who plan to sell to the government should be able to answer.

Although it would be ideal for a centralized agency like OMB, GSA, NIST, or GAO to adopt or publish such questionnaire(s), the primary goal should be for agencies to actually use and benefit from such a tool. That will require more than a top-down mandate to use a particular form – it will require advocacy and education for public administrators to be able to use the questionnaire effectively, and make better decisions based upon it.

- **Require legal review for all contracts that involve AI.** Contracting offices have standard operating procedures concerning internal approvals to address risks. Often, internal approvals are threshold-based (e.g., contracts in excess of $1 million) or trigger-based (e.g., sole-source contracts).[56]

  Given the novelty of legal risks and harms associated with AI, including copyright issues, privacy concerns, and the unique impact that vendors' standard intellectual property clauses may have on agencies' ability to explain and test AI systems, contracts involving AI should be reviewed by agency counsel with relevant expertise. This is additionally important to ensure consistency with the law, including civil rights laws, and compliance with the 2023 Racial Equity EO's mandate for agencies to acquire and use AI in a manner that advances equity. Agency counsel may also review a vendor's proposed means for testing for and remediating bias to ensure they are sufficient and comport with relevant legal requirements. Contracts that implicate personally identifiable information or government data should receive additional review and attention.

[56] *See, e.g.*, Homeland Security Acquisition Manual, *Subchapter 3004.70 Review and Approval of Proposed Contract Actions* (Oct 2009) which documents how DHS handles reviews https://www.dhs.gov/sites/default/files/publications/subchapter_3004.70_review_and_approval_of_proposed_contract_actions.pdf [https://perma.cc/P95J-ZC6A].

B. Include references to AI risks in the Federal Acquisition Regulations (FAR).

Although it is not actually necessary as a legal matter, the FAR Council[57] should consider making changes to provisions in the FAR to explicitly call out responsible AI practices — and policymakers should encourage them to do so. Among the parts that should be flagged for amendment are: Part 7 (Acquisition Planning); Part 10 (Market Research); Part 24 (Protection of Privacy and Freedom of Information); Part 39 (Acquisition of Information Technology); and Part 46 (Quality Assurance).

Any amendments would likely be useful if they provide specific references back to requirements in the 2023 AI Executive Order, the Final OMB AI Memo, the 2023 Racial Equity EO, and any applicable statutes, as well as guidance provided in NIST's AI Risk Management Framework and the Blueprint for an AI Bill of Rights. Additionally, because of the specific risks associated with "drift" (the ongoing efficacy and suitability of an AI model over time), there may be particularly useful changes in Part 46 (Quality Assurance) because traditional rules around acceptance – "acknowledgement that the supplies or services conform with applicable contract quality and quantity requirements"[58] – may not be sufficient to manage AI risks.

[57] The Federal Acquisition Regulatory Council is made up of GSA, NASA, and the Department of Defense (DOD) and, along with the Administrator of OFPP, is responsible to "jointly issue and maintain" the FAR.

[58] FAR, *Part 46.501* https://www.acquisition.gov/far/46.501 [https://perma.cc/KGK6-P48L].

C. Increase attention and capacity to perform pre-award vendor evaluation and post-award vendor monitoring through guidance and standardization.

A critical event in most procurements is vendor evaluation, when the government reviews offers from prospective vendors and selects the winning bidder. A hallmark of federal procurement is that the government must inform vendors of the method of evaluation before proposals are submitted and reviewed.[59]

In most cases, although vendor evaluations are heavily contested, the process works because there are objective criteria to evaluate bidders and select awardees. In the case of AI, however, relying on vendors’ *assertions* can be problematic because of the lack of independent research and evidence of vendor-provided AI products or the sufficiency of their risk management practices as described above. Additionally, relying exclusively on pre-award processes to ensure quality is problematic because AI systems can drift over time. This could potentially result in a system that does not work as intended and inflicts harm, which would only be known after the award is made and contract enacted.

As a result, one way to improve AI procurement outcomes would be to shift technical evaluations to earlier in the procurement process and attend to monitoring performance post-award, as required in the Final OMB AI Memo.[60] For example, the Department of

[59] 41 USC § 253a.

[60] Final OMB AI Memo, Sec. 5(d)(ii)(F).

Homeland Security's Procurement Innovation Lab has encouraged the use of "product or technical demonstrations"[61] to enable agencies to do hands-on testing of systems before they are procured. Individual federal agencies, ideally with more detailed support and guidance on procurement from OMB, should take the following actions to improve pre- and post-award procurement practices and policies:

- **Make broader use of their authority to conduct pre-award evaluations for AI models.** Although agencies have the authority to conduct technical evaluations before contract award, many agencies do not use "show, not tell" demonstrations or require rigorous, independent testing and evaluation strategies to eliminate vendors.

  GAO has explained, and comments on the Proposed OMB AI Memo have reinforced,[62] that government evaluation of AI should be iterative and that "to manage technical performance, AI technical stakeholders—data scientists, data engineers, developers, cybersecurity specialists, program managers, and others—will have to ensure that the AI system solves the problem initially identified; uses data sets appropriate for the problem; selects the most suitable algorithms; and evaluates and validates the system to ensure it is functioning as intended."[63]

  If a vendor is unable to meet the government's requirements, the government would be better off eliminating them pre-award. To accomplish this requires the government to conduct pre-award evaluations and technical demonstrations.

[61] Department of Homeland Security, *Procurement Innovation Lab Boot Camp Workbook*, Innovation Technique 2 (Oct 2019) https://www.dhs.gov/sites/default/files/publications/pil_boot_camp_workbook_oct_2019.pdf [https://perma.cc/55VL-KA5Q].

[62] Beeck Center for Social Impact and Innovation, *Comments to OMB on Proposed Memorandum on Agency Use of AI* (2023) https://beeckcenter.georgetown.edu/wp-content/uploads/2023/12/OMB_AI__Memo_Comment_Beeck_Center.pdf [https://perma.cc/TK22-8A6B].

[63] Government Accountability Office, *Artificial Intelligence: Key Practices to Help Ensure Accountability in Federal Use* (May 2023) https://www.gao.gov/assets/gao-23-106811.pdf [https://perma.cc/2BFF-ZUDF].

- **Further develop standards or certifications for responsible AI.** In general, acquisition professionals prefer as much clarity and certainty as possible when purchasing. The existence of a standard or a certification process can help make it easier for a procurement team to feel confident that a vendor is able to meet government requirements and prevent potential harms.

  Although it may be impossible to develop a certification process that ensures responsible AI, the government should encourage standardization around minimum expectations for vendors that provide AI-driven products. Two notable examples of enforcing standards in the technology domain are the use of **Voluntary Product Accessibility Templates** (VPATs) for compliance with Section 508 of the Rehabilitation Act[64] and the implementation of the **Federal Risk and Authorization Management Program** (FedRAMP) for cloud-service providers' compliance with NIST 800-53.[65]

  On the one hand, vendors use the VPAT to indicate that they conform with the accessibility requirements in an agency's solicitation. Many agencies even treat the submission of a VPAT itself as a formal solicitation requirement.[66] However, the VPAT is a self-certification, based on an industry-created form, and it is up to the agency to evaluate vendors' claims about their conformance with accessibility requirements and to monitor that the software conforms post-award through manual and automated testing.

[64] Section 508 generally requires that software be accessible and usable to individuals with disabilities. *See* https://www.section508.gov/sell/vpat/ [https://perma.cc/63QN-8JCN].

[65] National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations* (2020), defines the "information security standards and guidelines, including minimum requirements for federal information systems" https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final [https://perma.cc/7KXV-EJNF].

[66] *See, e.g.*, Government Accountability Office, *RK Consultancy Services, Inc*. (Nov 3, 2021) (denying a protest where "[t]he solicitation expressly required vendors to submit a VPAT in accordance with the completion instructions" and the protestor did not do so) https://www.gao.gov/products/b-420030%2Cb-420030.2 [https://perma.cc/7WPJ-6P7U].

At the opposite end of the spectrum, GSA operates FedRAMP, which was recently codified in the FedRAMP Authorization Act,[67] to provide a "standardized, reusable approach to security assessment and authorization for cloud computing products and services that process unclassified information used by agencies." Unlike the reliance on self-certification in VPATs, FedRAMP requires independent assessment of security controls by a Third Party Assessment Organization (3PAO), retained at the contractor's expense. Although FedRAMP is not typically a legal requirement at the outset of a contract, many agencies require that systems be approved by FedRAMP.

Building on top of the government's past efforts to enforce standards, the government should (at minimum) encourage the development of disclosure and certification standards and ensure ongoing conformance with those standards.

- **Build independent auditing into the acquisition process.** Agencies should consider creating a separate contract vehicle to independently audit and evaluate vendors' AI performance. Similar to the use of Independent Verification & Validation (IV&V) services[68] operated either generally through formal, centralized Program Management Offices[69] or specifically as contract actions

[67] James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, § 5921 *et seq.*

[68] According to the relevant IEEE standard, "Verification and validation (V&V) processes are used to determine whether the development products of a given activity conform to the requirements of that activity and whether the product satisfies its intended use and user needs." Institute of Electrical and Electronic Engineers, *1012-2016 - IEEE Standard for System, Software, and Hardware Verification and Validation* (2017) https://ieeexplore.ieee.org/document/8055462 [https://perma.cc/RWE9-CZH5].

[69] For example, NASA operates a PMO that provides IV&V services to other parts of the agency. NASA, IV&V Facility Services Overview (accessed Mar 29, 2024) https://www.nasa.gov/ivv-services-overview/ [https://perma.cc/2PE8-RDFK].

for individual projects or programs,[70] agencies should consider establishing formal methods to retain independent reviewers of vendors' AI claims.

Contracts should include regular reporting and auditing on system performance (including any emergent biases and efforts on bias mitigation), which would need to be included either as deliverables or explicit contract terms.[71]

D. Clarify and strengthen transparency, reporting, and oversight requirements and provide guidance to facilitate compliance.

A significant component of federal procurement policy is grounded in transparency, reporting, and oversight. There are strong norms and expectations within government around public transparency and reporting around technology acquisition and existing mechanisms – including, for example, formal notice-and-comment obligations under the Administrative Procedure Act – that can be

[70] See e.g., USASpending.gov, *Department of Veterans Affairs Blanket Purchase Agreement for IV&V for Medical Disability Program* (accessed April 11, 2024) https://www.usaspending.gov/award/CONT_IDV_36C10X22A0003_3600 [https://perma.cc/NU8C-WWFZ].

[71] Explicit contract terms could include requirements for ongoing testing, restrictions on secondary uses of data by both vendors and agencies, and transfer of ownership of procured systems to agencies. *Outsourced and Automated, supra* note 35, at 53-56.

leveraged to promote the responsible use of AI.[72] Further, the Final OMB AI Memo identifies particular minimum risk management practices that agencies must bear in mind during procurement. These practices include performing impact assessments prior to use, and ensuring ongoing monitoring, risk evaluation and mitigation, human training and oversight, notice and plain-language documentation, public consultation, and options to opt out of an AI system's functions in favor of a non-AI alternative.[73]

Critically, though, these mechanisms require a readily understood definition of AI and central bodies such as Congress, GAO, or OMB must provide clear guidance and requirements for agencies' disclosures and risk management practices.

- **Provide consistent guidance on the definition of AI systems subject to risk management processes in procurement.** As described above, the lack of a consistent and sufficiently expansive definition of AI reduces the ability of the government and the public to meaningfully evaluate agencies' use of AI.

  Congress should pass new legislation that broadens and improves the definition of AI to encompass the AI systems that undermine civil rights and democratic values. A more rigorous and inclusive definition codified by Congress would be the most effective approach – it would have the broadest reach across the federal government because it will become the new foundation for future legislative and executive actions on AI. However, in the interim OMB could offer further interpretation of the McCain NDAA definition of AI to ensure it captures all relevant systems. The authoritative legislative definition should avoid the errors of Executive Order 13960, which exempted AI embedded in "common commercial products," and in so doing

[72] Administrative Conference of the United States, *Agency Use of Artificial Intelligence, supra* note 13 ("When an AI system narrows the discretion of agency personnel, or fixes or alters the legal rights and obligations of people subject to the agency's action, affected people or entities might also sue on the ground that the AI system is a legislative rule adopted in violation of the APA's requirement that legislative rules go through the notice-and-comment process").

[73] Final OMB AI Memo, Sec. 5(c).

bypassed many applications that agencies may actually use.[74] A consistent definition would ensure more uniformity across agencies' AI inventories[75] and increase the likelihood of more responsive documentation pursuant to open records requests.[76] The inclusive, consistent definition of AI should also be the basis for guidance and procedures that agencies should develop for internal use about risk management mechanisms that should apply when acquiring and deploying AI.

- **Clarify and strengthen the federal government's AI inventories to provide greater transparency around agencies' use of AI systems.** As noted previously, transparency is an important governmental norm and a strong building block in responsible government use of AI. Executive Order 13960 created a requirement for agencies to inventory their "non-classified and non-sensitive use cases of AI" and publish those inventories publicly.[77] The agency AI inventories, which were then codified in the 2023 National Defense Authorization

[74] Definitions and standards may also improve transparency, *see* Anna Blue, *Federal Government AI Use Cases*, Responsible AI Institute (May 8, 2023) "Agencies need to standardize how and what they report in their inventories since the language, format, and depth of information varied tremendously across websites. For example, very few agencies reported the length of time the AI use case had been in operation, except for a few standout agencies like the Department of Interior. The Executive Order is not serving its purpose of increasing transparency into AI-driven operations if the public cannot understand how taxpayer money is being used to facilitate AI implementation" https://www.responsible.ai/federal-government-ai-use-cases/ [https://perma.cc/2C3G-3L4Q].

[75] Bowman Cooper, *Like Looking for a Needle in an AI-Stack*, Center for Democracy & Technology (July 21, 2023), https://cdt.org/insights/like-looking-for-a-needle-in-an-ai-stack/ [https://perma.cc/UFG7-LNVB].

[76] *Outsourced and Automated, supra* note 35.

[77] The carveout of classified- and sensitive-use cases has come under recent criticism. *See* Blue, *supra* note 71 ("[T]he database is not wholly representative of agency AI use cases, since some use cases might not be disclosed to the public. The Department of Transportation, for instance, had three rows in their inventory labeled as "redacted," which might have been due to information security concerns. Four agencies (HUD, USAID, NIST, and NSF) claimed on their websites not to use AI in their operations or to have identified no 'relevant' AI use cases. It is difficult to believe that the NIST does not use AI in its projects, but if it truly does not, why is that? It is possible that none of the NIST use cases were considered non-classified and non-sensitive. It is also possible that the federal government needs to encourage better information- and resource-sharing between agencies so that AI-driven tools are appropriately exchanged and distributed.").

Act and elaborated upon in the Final OMB AI Memo, could provide significant transparency to the public around the federal government's use of AI, but they are currently falling short of that ideal.[78]

OMB should issue clear and specific directives to agencies to ensure the AI inventories achieve their potential. It should clarify agencies' obligations to disclose AI uses and provide more specificity about permissible exceptions to those obligations.[79] OMB should also review agencies' determinations that systems may be exempt from public disclosure, and challenge and correct overbroad interpretations where they are identified.[80] Further, OMB should ensure that the inventories from various agencies are accessible via a single interface that is easily navigable and interoperable, with past entries archived, and should provide (or ensure that agencies provide) notice when updates are made.[81]

- **Add specific reporting requirements regarding responsible AI procurement and management in the Federal Information Technology Acquisition Reform Act (FITARA) scorecard.**[82] FITARA has been a major driver in moving agencies to adopt the commercial cloud because of the visibility of the FITARA scorecard, which uses a simple grading method to track how well agencies are complying with FITARA's requirements to manage their IT adoption. Including metrics that reflect responsible AI practices in the FITARA scorecard (e.g., "percent of systems that have independent algorithmic impact assessments") could induce CIOs to prioritize responsible AI practices and policies.

[78] Center for Democracy & Technology, *Comment to OMB on Proposed Memorandum on Agency Use of AI, supra* note 6; Christie Lawrence et al., *The Bureaucratic Challenge to AI Governance: An Empirical Assessment of Implementation at U.S. Federal Agencies*, AAAI/ACM Conference on AI, Ethics, and Society (2023), https://dl.acm.org/doi/pdf/10.1145/3600211.3604701 [https://perma.cc/TDN3-GRPZ]; Beeck Center, *supra* note 60.

[79] *Civil Rights Organizations Identify Priorities for OMB Memo on Agency Use of AI, supra* note 24.

[80] For further recommendations on the AI Inventory, see Center for Democracy & Technology, *Comment to OMB on Proposed Memorandum on Agency Use of AI, supra* note 6.

[81] *Id.*

[82] Government Accountability Office, *Information Technology: Biannual Scorecards Have Evolved and Served as Effective Oversight Tools* (Jan 20, 2022) https://www.gao.gov/products/gao-22-105659 [https://perma.cc/D4T2-DBBG].

Although the FITARA scorecard is maintained by the House's Subcommittee on Government Operations, Committee on Oversight and Reform, the "data used for grading federal agencies have largely been publicly available and regularly updated."[83] Agreeing upon what metrics should go into a scorecard would likely require coordination between the Subcommittee, GAO, and OMB. This may be a promising opportunity given GAO's prior work on the AI Accountability Framework, and OMB's current work on guidance for both agency use and agency procurement of AI. Further, the 2023 AI EO requires OMB to develop a method for agencies to "track and assess their ability to adopt AI into their programs and operations [and] manage its risks," addressing the practices and capabilities needed for AI governance across IT infrastructure, risk management, and other areas.[84]

- **Develop guidance and a consistent approach to intellectual property provisions in vendor contracts, to ensure such provisions do not inappropriately limit government agencies' abilities to test, explain, and audit AI systems.** In a growing number of cases, government agencies have been blocked from disclosing necessary information for outside testing and validation of their AI systems because of vendors' assertions of trade secrets.[85] Without effective contract terms governing this issue, agencies risk being limited in their ability to explain, test, or independently validate AI tools and systems, undermining responsible use processes and potentially creating legal problems for the agency down the road.

[83] *Id.*

[84] 2023 AI EO, Sec. 10.2(c).

[85] *See, e.g.*, Rebecca Wexler, *It's Time to End the Trade Secret Evidentiary Privilege Among Forensic Algorithm Vendors*, Brookings Institute (July 13, 2021) https://www.brookings.edu/articles/its-time-to-end-the-trade-secret-evidentiary-privilege-among-forensic-algorithm-vendors/ [https://perma.cc/AET3-VD66]; Cary Coglianese, *AI, Due Process, and Trade Secrets*, The Regulatory Review (Sep 4, 2023) https://www.theregreview.org/2023/09/04/coglianese-ai-due-process-and-trade-secrets/ [https://perma.cc/8U6K-38EL].

ACUS has expressly cautioned against this risk, noting that:

"When agencies' AI systems rely on proprietary technologies or algorithms the agencies do not own, the agencies and the public may have limited access to the information about the AI techniques. Agencies should strive to anticipate such circumstances and address them appropriately, such as by working with outside providers to ensure they will be able to share sufficient information about such a system. Agencies should not enter into contracts to use proprietary AI systems unless they are confident that actors both internal and external to the agencies will have adequate access to information about the systems."[86]

Express guidance or directives from OMB, ACUS, or another well-positioned expert agency would help procurement officers identify and navigate this risk, as well as establishing a recognized "best practice" for officers to invoke in contract negotiations.

- **Develop and publish an "oversight guide" for reviewing agency acquisition activities.** Building on the GAO's "Accountability Framework for Federal Agencies and Other Entities,"[87] the Congressional Research Service or agencies responsible for oversight like GAO or OMB should develop an "oversight guide" with specific references to parts of the acquisition planning process where agencies should *already* be considering responsible AI principles.[88]

  An oversight guide could be used by Congress, federal agency executives, inspectors general, civil society, and the public to better understand what types of questions to ask of federal government employees and federal contractors. Because structured oversight processes can help drive agencies toward better outcomes, having a shared understanding of what "good" looks like from an oversight perspective would be useful.

[86] Administrative Conference of the United States, *Agency Use of Artificial Intelligence, supra* note 13.

[87] GAO AI Accountability Framework, *supra* note 14.

[88] Beeck Center, *supra* note 60.

Although an oversight guide would ideally come from the federal government, non-government or civil society organizations can also help create an oversight guide for AI that can encourage beneficial agency practices.

- **Strengthen requirements for agencies to conduct algorithmic impact assessments and require agencies to publish them on their websites.** Agencies are required by law[89] to conduct Privacy Impact Assessments (PIAs) when "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form" and publish them on the agency's website. To help agencies fulfill this privacy impact requirement with respect to their AI practices, the 2023 AI EO also requires OMB to issue a request for information "seek[ing] feedback regarding how privacy impact assessments may be more effective at mitigating privacy risks, including those that are further exacerbated by AI," and "to support and advance the near-term actions and long-term strategy identified" through this feedback.[90]

  OMB has advised that a PIA must be written in "plain language" and address "how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks."[91]

[89] Section 208(e) of the E-Government Act of 2002, Pub. L. No. 107-347, 44 U.S.C. § 3501 note.

[90] 2023 AI EO, Sec. 9(a)(iii)-(iv).

[91] Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept 26, 2003) https://obamawhitehouse.archives.gov/omb/memoranda_m03-22/ [https://perma.cc/39BX-Z2US].

Similarly, agencies should conduct algorithmic impact assessments (AIAs) —either as part of the PIA process or as a standalone assessment—whenever an automated system is used to make or influence a decision that has a service-delivery impact. The Final OMB AI Memo requires AI impact assessments as a minimum risk management practice for rights- or safety-impacting systems (covering the majority of instances where a PIA would be required), but it does not require the results of the AIA to be made public. These AIAs must include the intended purpose, expected benefits, potential risks of the AI use, and the quality and appropriateness of the data used in the AI system.[92] When completing AIAs, agencies should also be required to include both general and sector-specific impacts and details about non-AI approaches that were considered, and should be required to publish their AIAs for each of their AI use cases in a manner that is easy to find through their AI inventory submissions.[93] A published AIA should provide sufficient detail and raw figures for the public to understand how the AI was trained, its outcomes for each affected demographic group, and how the agency measures the impacts on these groups.[94]

Such a requirement would create accountability among agencies and vendors to consider and document risks associated with the adoption of AI.

- **Encourage NIST to adopt a standard for AIAs.** Although there have been legislative proposals describing what should be included in an AIA,[95] no formal standard describes what

[92] Final OMB AI Memo, Sec. 5(c)(iv)(A).

[93] CDT, *Comments to OMB on Proposed Memorandum for Agency Use of AI, supra* note 6, at 8-9 and 23.

[94] *Id.* at 23.

[95] *See, e.g.*, S.3572, Algorithmic Accountability Act of 2022 https://www.congress.gov/bill/117th-congress/senate-bill/3572/text#id2676B8898BB34E74A094B8CA5BF153BD.

should go into an AIA. Although NIST has adopted the AI RMF, it should go further to develop a standard for federal AIAs (akin to NIST FIPS 199 [Standards for Security Categorization of Federal Information and Information Systems] / SP 800-53 [Security and Privacy Controls for Information Systems and Organizations]), ideally with different levels associated with the degree of impact (akin to the FIPS 199 low/moderate/high impact approach). Any such standard must incorporate input from all affected stakeholders, including civil rights groups and impacted communities.

E. Increase federal workforce capacity to ensure agencies are prepared to evaluate and manage risks throughout AI procurement.

To address the currently limited capacity of the federal workforce to meaningfully support or critically evaluate AI acquisitions, better training and learning opportunities for federal employees and support programs are needed to improve the government's socio-technical capacity to manage AI.[96] These programs should be monitored and supported by the AI and Technology Talent Task Force required by the 2023 AI EO.[97] Individual agencies should prioritize this work now as they take steps to procure AI-driven technology, while centralized policymaking and resourcing bodies like OMB coordinate with USDS and GSA to connect agencies to the expertise needed for sufficient training on responsible AI.

[96] Partnership for Public Service, *Comment to OMB on Proposed Memorandum on Agency Use of AI* (Dec 6, 2023), https://ourpublicservice.org/publications/max-stiers-public-comments-on-ombs-advancing-governance-innovation-and-risk-management-for-agency-use-of-artificial-intelligence-draft-memorandum-guidance/ [https://perma.cc/TAA7-SYFS].

[97] 2023 AI EO, Sec. 10.2 (b)-(c).

- **Develop training modules that ideally would be incorporated into the existing procurement curriculum.** The 2023 AI EO requires each agency to implement (or expand existing) AI training programs for their workforce.[98] Although standalone training modules could be helpful, they are more likely to affect federal procurement practices and policies if they are embedded in training opportunities and curricula that are already in use.

  For example, the Digital IT Acquisition Profession (DITAP) program uses a cohort model to teach "federal government acquisition professionals to design innovative and flexible procurements for IT/Digital Services, and how to become change ambassadors."[99] Working with United States Digital Service (USDS), the Office of Federal Procurement Policy (OFPP), and DITAP providers to incorporate responsible AI concepts into the DITAP curriculum would have a broad reach among acquisition professionals who plan to work with digital services teams.

  Similarly, civil society organizations also offer training programs that could benefit from the inclusion of information about how federal leaders can responsibly procure AI.[100] Partnering with these organizations to incorporate responsible AI training into the Federal Acquisition Institute curriculum will help reach acquisition professionals (including Contracting Officers and their representatives).

- **Encourage growth and support of digital services teams within the government with experience designing and deploying responsible AI.** A number of organizations within the government are focused on recruiting, developing, and retaining technical talent that can bring focused capacity to some of the larger challenges within the federal procurement ecosystem. For

[98] 2023 AI EO, Sec. 10.2(g).

[99] United States Digital Services TechFAR Hub, *Digital IT Acquisition Professional Training Program* (accessed Mar 29, 2024) https://techfarhub.usds.gov/get-started/ditap/ [https://perma.cc/9NW9-VSYZ].

[100] *See, e.g.,* Partnership for Public Service, AI Federal Leadership Program (accessed Mar 21, 2024) https://ourpublicservice.org/course/ai-federal-leadership-program/ [https://perma.cc/6XLH-RSDV].

example, the US Digital Service, the GSA CoE, Senior Advisors for Delivery, and the Presidential Innovation Fellows programs all bring technical expertise to assist agencies in their missions.[101] These programs would benefit from the inclusion of training and information on AI, including its responsible procurement.

[101] National Artificial Intelligence Advisory Committee, Recommendations: AI's Procurement Challenge (Oct 2023) https://ai.gov/wp-content/uploads/2023/11/Recommendations_AIs-Procurement-Challenge.pdf [https://perma.cc/6JM4-HB4E].

06 Conclusion

As the federal government continues to pursue AI adoption and responsible AI use as part of service delivery, the procurement process presents a unique opportunity to promote greater deliberation by government actors about the risks inherent to AI. The 2023 AI EO, Final OMB AI Memo, and 2023 Racial Equity EO set forth an important commitment to effective, equitable, and ethical use of AI by the federal government, and procurement frameworks will be a key component of ensuring their promise is made real. Existing IT acquisition processes can be adapted to bring focus to mitigating AI-specific risks, and enable the government to challenge unsubstantiated claims by vendors and ensure strong post-award management practices.

Such work will require continued executive commitment to responsible AI practices, an investment in much-needed socio-technical capacity, and a healthy amount of skepticism about AI's techno-solutionist claims. Failing to address those needs creates significant risk of public harm and waste of taxpayer dollars. Fortunately, there are clear opportunities for meaningful interventions, and a community of individuals inside and outside of government who understand the stakes.

07 Appendix A: History of Approaches to Federal AI Procurement

As noted in Section II, "A Brief History of Federal AI Governance," the last several years have seen a slew of activity from the federal government concerning the use of AI, ranging from congressional actions to executive orders to agency-specific guidance for use.

Figures 1 and 2 illustrate the growth in attention paid to AI. Many of these actions explicitly address the procurement of AI systems, while others impact procurement by managing government use of AI, meaning agencies must ensure that procured systems are able to meet the requirements. This appendix expands on Section II, providing a non-exhaustive timeline of federal government actions on AI.

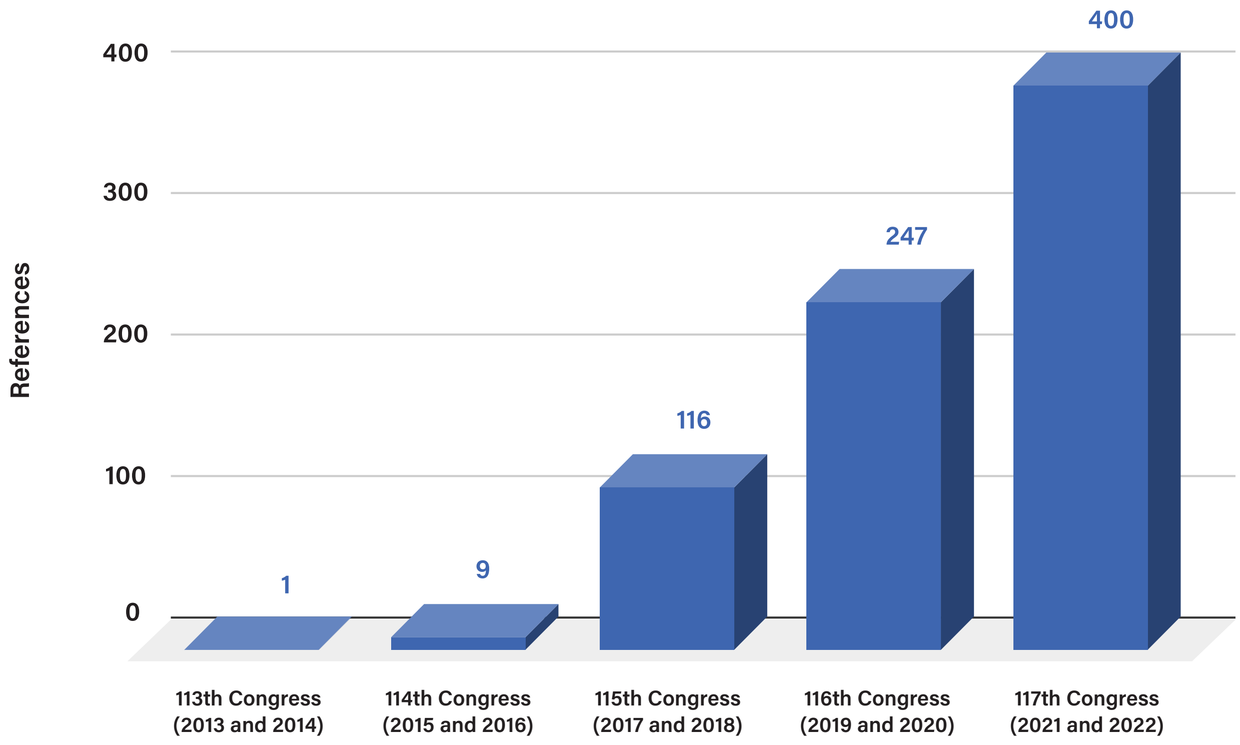

Figure 1. References in the Congressional Record to "artificial intelligence."

A bar chart showing that references to the term "artificial intelligence" in the Congressional Record have grown from nine references in the 114th Congress (2015-2016) to 400 references in the 117th Congress (2021-2022), demonstrating that Congress has significantly increased its attention on artificial intelligence over the last three congressional periods.

Source: *https://www.congress.gov/*

2018-2019 Federal Actions

As mentioned previously, among the earliest federal government actions related to AI was contained in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 ("McCain NDAA"),[102] enacted in 2018 during the 115th Congress. Section 238 of the McCain NDAA established the Joint Artificial Intelligence Center and notably included the first legislative definition of AI. In subsequent legislative and executive actions, that definition often has been incorporated by reference.

Shortly after the McCain NDAA, President Trump took the first major executive action, signing Executive Order 13859 on Maintaining American Leadership in Artificial Intelligence on

[102] *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, Pub. L. No. 115–232 https://www.congress.gov/bill/115th-congress/house-bill/5515.

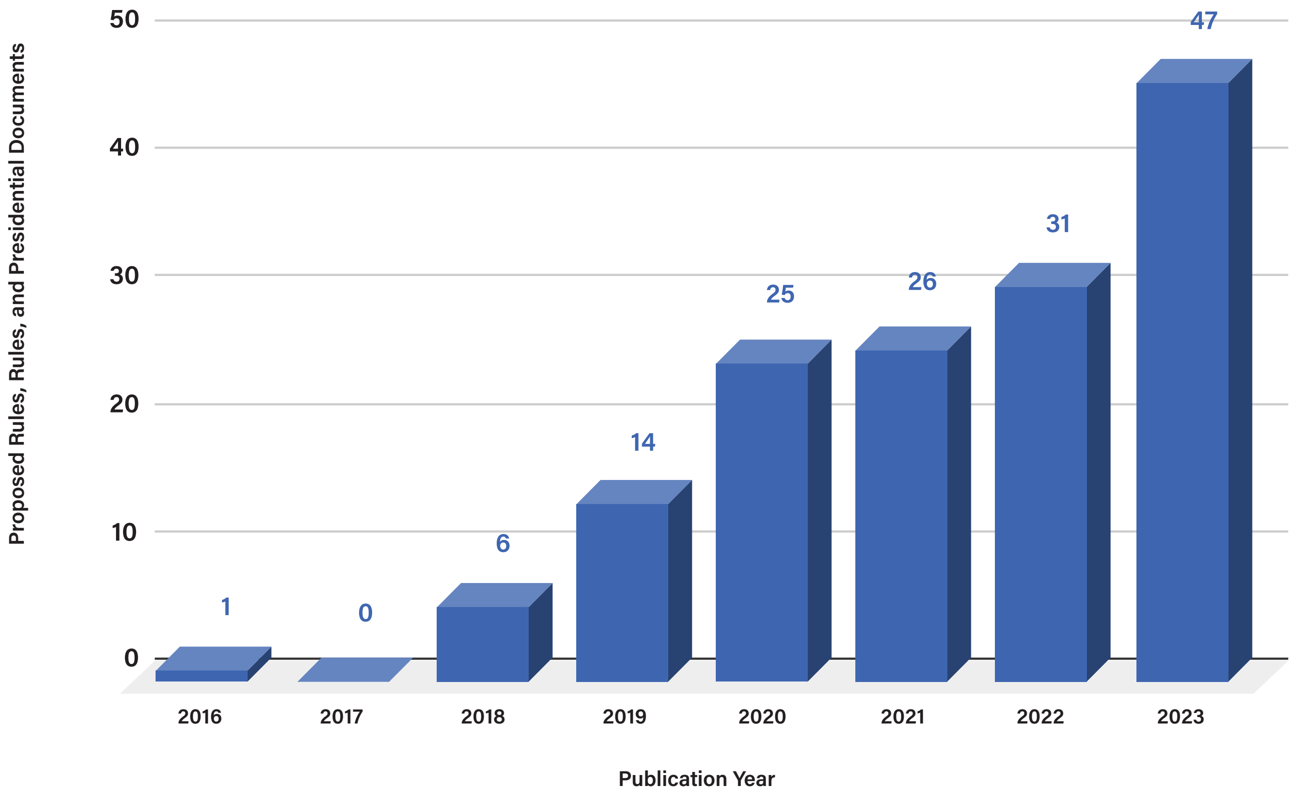

Figure 2. Actions in the Federal Register referring to "artificial intelligence."

A bar graph showing the growth in rules, proposed rules, and presidential documents from 2016 to 2023. Notably, although no presidential action had contained the phrase "artificial intelligence" until 2018, there have been at least 20 presidential actions, including several executive orders tallied here, since then.

Source: *https://www.federalregister.gov/*

February 11, 2019,[103] which set forth the "policy of the United States Government to sustain and enhance the scientific, technological, and economic leadership position of the United States in AI R&D and deployment." It took a coordinated Federal Government strategy, the American AI Initiative (Initiative), guided by five principles:

> *"(a) The United States must drive technological breakthroughs in AI across the Federal Government, industry, and academia in order to promote scientific discovery, economic competitiveness, and national security.*

[103] *Executive Order 13859 on Maintaining American Leadership in Artificial Intelligence* (Feb 11, 2019) https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence [https://perma.cc/USK9-BVNG].

> *"(b) The United States must drive development of appropriate technical standards and reduce barriers to the safe testing and deployment of AI technologies in order to enable the creation of new AI-related industries and the adoption of AI by today's industries.*
>
> *"(c) The United States must train current and future generations of American workers with the skills to develop and apply AI technologies to prepare them for today's economy and jobs of the future.*
>
> *"(d) The United States must foster public trust and confidence in AI technologies and protect civil liberties, privacy, and American values in their application in order to fully realize the potential of AI technologies for the American people.*
>
> *"(e) The United States must promote an international environment that supports American AI research and innovation and opens markets for American AI industries, while protecting our technological advantage in AI and protecting our critical AI technologies from acquisition by strategic competitors and adversarial nations."*

2020 Federal Actions

As noted in Section II, the 116th Congress saw the enactment of the National Artificial Intelligence Initiative Act of 2020[104] and the AI in Government Act of 2020,[105] which established the National AI Initiative and the AI Center of Excellence, respectively. The purpose of the National AI Initiative legislation was primarily to coordinate research and development activities across federal agencies, and

[104] *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, Pub. L. No. 116–283 https://www.congress.gov/bill/116th-congress/house-bill/6395.

[105] *Consolidated Appropriations Act*, 2021, Pub. L. No. 116–260 https://www.congress.gov/bill/116th-congress/house-bill/133.

established the National AI Initiative Office within the Office of Science and Technology Policy. Meanwhile, the AI in Government Act aimed to encourage the adoption of AI by federal agencies.

Notably, the AI in Government Act also required the Office of Management and Budget (OMB) to "issue a memorandum to the head of each agency that shall—

> *"(1) inform the development of policies regarding Federal acquisition and use by agencies regarding technologies that are empowered or enabled by artificial intelligence, including an identification of the responsibilities of agency officials managing the use of such technology;*
>
> *"(2) recommend approaches to remove barriers for use by agencies of artificial intelligence technologies in order to promote the innovative application of those technologies while protecting civil liberties, civil rights, and economic and national security;*
>
> *"(3) identify best practices for identifying, assessing, and mitigating any discriminatory impact or bias on the basis of any classification protected under Federal nondiscrimination laws, or any unintended consequence of the use of artificial intelligence, including policies to identify data used to train artificial intelligence algorithms as well as the data analyzed by artificial intelligence used by the agencies; and*
>
> *"(4) provide a template of the required contents of the agency plans described in subsection (c)."*

Although the AI in Government Act required that guidance be issued in September 2021, OMB did not issue the directed guidance at that time. OMB did ultimately release draft guidance for public comment in November 2023, as part of the suite of actions following Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (discussed in more detail in Section III and further in this section), which covered much of the ground directed by the AI in Government Act.[106]

[106] Final OMB AI Memo.

As directed by Executive Order 13859, the Director of OMB issued M-21-06, "Guidance for Regulation of Artificial Intelligence Applications,"[107] which prescribed "policy considerations that should guide, to the extent permitted by law, regulatory and non-regulatory approaches to AI applications developed and deployed outside of the Federal government." This memorandum, however, explicitly stated that government uses of AI were out of scope for this guidance.

Shortly thereafter, as discussed previously, on December 3, 2020, President Trump signed Executive Order 13960 on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government (Executive Order 13960),[108] which set forth a "policy of the United States to promote the innovation and use of AI, where appropriate, to improve Government operations and services in a manner that fosters public trust, builds confidence in AI, protects our Nation's values, and remains consistent with all applicable laws, including those related to privacy, civil rights, and civil liberties."

Executive Order 13960 also established several "principles" for agencies to follow when "designing, developing, acquiring, and using AI in the Federal Government," including: "Lawful and respectful of our Nation's values;" "Purposeful and performance-driven;" "Accurate, reliable, and effective;" "Safe, secure, and resilient;" "Understandable:" "Responsible and traceable;" "Regularly monitored;""Transparent;" and "Accountable."

Finally, this order required agencies to identify a "responsible official" to "coordinate implementation of the Principles...with the Agency Data Governance Body."

[107] Office of Management and Budget, *Guidance for Regulation of Artificial Intelligence Applications* (Nov 17, 2020) https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf [https://perma.cc/22BC-D3N8].

[108] Executive Order 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government* (Dec 2020) https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government [https://perma.cc/P5SD-NWFZ].

Closing out 2020, the Administrative Conference of the United States (ACUS) issued a December 2020 recommendation on "Agency Use of Artificial Intelligence,"[109] which provided broad-ranging guidance to agencies about the use of AI. With regard to procurement specifically, ACUS noted that:

> *Decisions about whether to obtain an AI system can involve important trade-offs. Obtaining AI systems from external sources might allow agencies to acquire more sophisticated tools than they could design on their own, access those tools sooner, and save some of the up-front costs associated with developing the technical capacity needed to design AI systems. Creating AI tools within agencies, by contrast, might yield tools that are better tailored to the agencies' particular tasks and policy goals. Creating AI systems within agencies can also facilitate development of internal technical capability, which can yield benefits over the lifetime of the AI systems and in other technological tasks the agencies may confront.*
>
> *Certain government offices*[110] *are available to help agencies with decisions and actions related to technology. Agencies should make appropriate use of these resources when obtaining an AI system. Agencies should also consider the cost and availability of the technical support necessary to ensure that an AI system can be maintained and updated in a manner consistent with its expected life cycle and service mission.*

[109] Administrative Conference of the United States, *Agency Use of Artificial Intelligence, supra* note 13.

[110] Referring to 18F and USDS.

2021 Federal Actions

In 2021, a number of federal agencies issued guidance and documentation on the use of AI, including AI strategies from the Department of Health and Human Services (HHS) and the Department of Veterans Affairs (VA),[111] and guidance from the Department of Defense (DoD).[112] Additionally, the Government Accountability Office (GAO) published GAO-21-519SP, An Accountability Framework for Federal Agencies and Other Entities, addressing four principles of "governance, data, performance, and monitoring."[113] The framework describes practices for federal agencies as they select and implement AI systems, including questions for vendors, auditors, and third-party assessors to consider in evaluating the systems.

2022 Federal Actions

Returning to legislation, the 117th Congress enacted the Advancing American AI Act[114] and the Training for the Acquisitions Workforce Act (AI Training Act), as mentioned in Section II.[115] In the Advancing

[111] Department of Health and Human Services, *Artificial Intelligence (AI) Strategy* (Jan 2021) https://www.hhs.gov/sites/default/files/final-hhs-ai-strategy.pdf [https://perma.cc/Z6UM-XN7Z]; Department of Veterans Affairs, *Artificial Intelligence (AI) Strategy* (July 2021) https://www.research.va.gov/naii/VA_AI_Strategy_V2-508.pdf [https://perma.cc/G2L4-5YWE].

[112] Department of Defense, *Implementing Responsible Artificial Intelligence in the Department of Defense* (May 26, 2021) https://media.defense.gov/2021/May/27/2002730593/-1/-1/0/implementing-responsible-artificial-intelligence-in-the-department-of-defense.pdf [https://perma.cc/BBH4-6YN4].

[113] GAO AI Accountability Framework, *supra* note 14.

[114] *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, Pub. L. No. 117-263 https://www.congress.gov/bill/117th-congress/house-bill/7776.

[115] *AI Training Act*, Pub. L. No. 117-207 https://www.congress.gov/bill/117th-congress/senate-bill/2551.

American AI Act, Congress renewed the push for OMB guidance on AI, and further required that OMB develop an initial means to:

> *"(A) ensure that contracts for the acquisition of an artificial intelligence system or service—*
>
> > *"(i) align with the guidance issued to the head of each agency under section 104(a) of the AI in Government Act of 2020 (title I of division U of Public Law 116–260);*
> >
> > *"(ii) address protection of privacy, civil rights, and civil liberties;*
> >
> > *"(iii) address the ownership and security of data and other information created, used, processed, stored, maintained, disseminated, disclosed, or disposed of by a contractor or subcontractor on behalf of the Federal Government; and*
> >
> > *"(iv) include considerations for securing the training data, algorithms, and other components of any artificial intelligence system against misuse, unauthorized alteration, degradation, or rendering inoperable; and*
>
> *"(B) address any other issue or concern determined to be relevant by the [OMB] Director to ensure appropriate use and protection of privacy and Government data and other information."*

The AI Training Act required OMB and the General Services Administration (GSA) to "develop and implement or otherwise provide an AI training program for the covered workforce" to "ensure that the covered workforce has knowledge of the capabilities and risks associated with AI" within a year of the law's enactment on October 17, 2022.

In October 2022, the Office of Science and Technology Policy published the Blueprint for an AI Bill of Rights (Blueprint), which established "five principles and associated practices to help guide the design, use, and deployment of automated systems to protect the rights of the American public in the age of artificial intelligence."[116] The five principles are: "Safe and Effective Systems;" "Algorithmic Discrimination Protections;" "Data Privacy;" "Notice and Explanation;" and "Human Alternatives, Consideration, and Fallback." As noted previously, the Blueprint contains extensive information on understanding and mitigating AI harms.

Also in 2022, ACUS published recommendations concerning agencies' use of Automated Legal Guidance,[117] based on agencies' increased use of automation of "legal guidance to the public through online tools and other technologies" such as the IRS's "Interactive Tax Assistant" and the United States Citizenship and Immigration Services's interactive chatbot "Emma."[118] (ACUS has similarly issued guidance to agencies on navigating the risk of mass, computer-generated, and falsely attributed comments in agency proceedings,[119] and on the use of AI for retrospective review of agency rules.[120])

[116] White House Office of Science and Technology Policy, Blueprint for an AI Bill of Rights, *supra* note 18.

[117] Administrative Conference of the United States, *Automated Legal Guidance at Federal Agencies*, *supra* note 13.

[118] *Id.*

[119] Administrative Conference of the United States, *Managing Mass, Computer-Generated, and Falsely Attributed Comments* (June 2021) https://www.acus.gov/sites/default/files/documents/Final%20-%20Managing%20Mass%20Computer-Generated%20and%20Falsely%20Attributed%20Comments.pdf [https://perma.cc/CE56-ALAP].

[120] Administrative Conference of the United States, *Using Algorithmic Tools in Retrospective Review of Agency Rules* (June 2023) https://www.acus.gov/sites/default/files/documents/2023-3%20Algorithmic%20Tools%20in%20Retrospective%20Review%20Final.pdf [https://perma.cc/6EGS-YTJT].

2023 Federal Actions

In early 2023, NIST published the AI Risk Management Framework (AI RMF), which is "intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems."[121] The AI RMF is "complementary" to the Blueprint[122] and is intended to "be applied across a wide range of perspectives, sectors, and technology domains, and should be universally applicable to any AI technology or use case."[123]

The AI RMF includes sections that frame the risks of AI: "articulates the characteristics of trustworthy AI and offers guidance for addressing them," "describes expected benefits for users of the framework," and "provides outcomes and actions that enable dialogue, understanding, and activities to manage AI risks and responsibility develop trustworthy AI systems." The AI RMF anticipates the development of "use-case Profiles" which "are implementations of the AI RMF functions, categories, and subcategories for a specific setting or application based on the requirements, risk tolerance, and resources of the Framework user."[124]

The Biden White House's first action on AI came in Executive Order 14091 on Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government (2023

[121] AI RMF, *supra* note 12.

[122] Remarks by Dr. Alondra Nelson, Launch of the NIST AI Risk Management Framework (Jan 26, 2023) https://www.whitehouse.gov/ostp/news-updates/2023/01/26/remarks-for-dr-alondra-nelson-at-the-launch-of-the-nist-ai-risk-management-framework/ [https://perma.cc/2XTC-BMLV].

[123] Remarks by Laurie E. Locascio, Launch of the NIST AI Risk Management Framework (Jan 26, 2023) https://www.nist.gov/speech-testimony/launch-nist-ai-risk-management-framework [https://perma.cc/E8LY-2MNJ].

[124] AI RMF, *supra* note 12.

Racial Equity EO).[125] Among other things, the 2023 Racial Equity EO mandates that "[w]hen designing, developing, acquiring, and using artificial intelligence and automated systems in the Federal Government, agencies shall do so, consistent with applicable law, in a manner that advances equity."[126] Additionally, this order requires agencies to "ensure that their respective civil rights offices are consulted on decisions regarding the design, development, acquisition, and use of artificial intelligence and automated systems."

The 2023 Racial Equity EO was followed in October 2023 by Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (2023 AI EO. In addition to the requirements referenced earlier, the 2023 AI EO also sets forth agency-specific requirements – for example, directing the Department of Justice to conduct a review of the use of AI in the criminal justice system, and the Departments of Health and Human Services and Agriculture to develop plans, issue guidance, or otherwise use their civil rights authorities to "address[] the use of automated or algorithmic systems in the implementation by States and localities of public benefits and services" and prevent and address harms resulting from such uses.[127]

The 2023 AI EO expressly incorporates both the Blueprint and the AI RMF by reference, stating that OMB should establish for federal agencies "required minimum risk-management practices for Government uses of AI that impact people's rights or safety, including, where appropriate, the following practices derived from the Blueprint and the AI RMF: "conducting public consultation,

[125] Executive Order 14091 On Advancing Racial Equity and Support for Underserved Communities Through the Federal Government (Feb 16, 2023), https://www.whitehouse.gov/briefing-room/presidential-actions/2023/02/16/executive-order-on-further-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government/ [https://perma.cc/GTG2-CGVG].

[126] *Id.* at Sec. 4(b).

[127] *Id.* at Sec. 7.2(b).

assessing data quality, assessing and mitigating disparate impacts and algorithmic discrimination, providing notice of the use of AI, continuously monitoring and evaluating deployed AI, and granting human consideration and remedies for adverse decisions made using AI."

Finally, on November 3, 2023, OMB issued its Proposed Memorandum on Agency Use of AI, which, as noted previously, provides agencies with explicit though high-level, guidance on procuring AI systems, as well as guidance on the use of AI systems that will inform how agencies will need to assess vendor systems. This was followed by a final version on March 28, 2024.[128]

[128] Final OMB AI Memo, *supra* note 3.

08 Appendix B: AI Risks Compared To Traditional Software Risks

The **AI RMF Appendix's "How AI Risks Differ from Traditional Software Risks"**[129] offers a helpful starting point from which to identify unique procurement challenges presented by AI.

The table on the next page summarizes some of these AI-specific risks and how they might affect the procurement process.

[129] AI RMF, Appendix B, *supra* note 12.

Table 1. AI-specific risks and how they might affect the procurement process.

From the NIST AI RMF Appendix's "How AI Risks Differ from Traditional Software Risks."

How NIST characterizes the AI-specific risk:	How the risk might affect the procurement process:
The data used for building an AI system may not be a true or appropriate representation of the context or intended use of the AI system, and the ground truth may either not exist or not be available. Additionally, harmful bias and other data quality issues can affect AI system trustworthiness, which could lead to negative impacts.	A hallmark principle of public procurement is that up-front competition will lead to the best vendor selection, but adequate testing and monitoring of a solution in production will need to be built into procurement processes because full evaluation is not possible ex ante or based on a static evaluation of proposed solutions.
Intentional or unintentional changes during training may fundamentally alter AI system performance.	Procurement rules require formal processes (such as change orders or modifications) to address changes after "acceptance" of a service or supply. These processes should be triggered when intentional changes are made, and when unintentional changes are detected or suspected due to system performance.
Datasets used to train AI systems may become detached from their original and intended context or may become stale or outdated relative to deployment context.	Procurements are often structured toward the creation of long-term contracts (typically, 5 years). Retraining AI will need to be built into procurements. If agencies procure systems from other agencies, this may add to the risk of systems becoming detached from their intended contexts.
AI systems may require more frequent maintenance and triggers for conducting corrective maintenance due to data, model, or concept drift.	Without effective management practices, there is a significant likelihood that "Operations and Maintenance" budgets will compete with "Development, Modernization, and Enhancement" budgets or incentivize agencies to underinvest in post-award monitoring and improvement.
Increased opacity and concerns about reproducibility.	A lack of transparency can create distrust and prevent accountability between government and industry and harm the public's trust in government. Appropriate transparency and explainability requirements will need to be built into contracts with internal technical expertise to analyze disclosures. Companies' intellectual property protections can often pose a barrier.

Table 1 (continued). AI-specific risks and how they might affect the procurement process.

From the NIST AI RMF Appendix's "How AI Risks Differ from Traditional Software Risks."

How NIST characterizes the AI-specific risk:	How the risk might affect the procurement process:
Difficulty in performing regular AI-based software testing, or determining what to test, since AI systems are not subject to the same controls as traditional code development.	Structuring procurements with appropriate evaluation criteria is already difficult. Developing and tailoring appropriate evaluation criteria for AI (and accurately assessing proposals against those criteria) will require additional technical capacity within the government.
Inability to predict or detect the side effects of AI-based systems beyond statistical measures.	Without mature post-award governance models, it may not be clear who has the legal and financial burden to deal with unintended consequences.

09 Appendix C: Glossary Of Acronyms and Abbreviations

2023 AI EO

Executive Order 14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

ACUS

Administrative Conference of the United States

https://www.acus.gov/

AI RMF

AI Risk Management Framework

https://www.nist.gov/itl/ai-risk-management-framework

AI Training Act

Artificial Intelligence Training for the Acquisition Workforce Act

https://www.congress.gov/bill/117th-congress/senate-bill/2551

Blueprint

Blueprint for an AI Bill of Rights

https://www.whitehouse.gov/ostp/ai-bill-of-rights/

CPARS

Contractor Performance Assessment Reporting System

https://www.cpars.gov/

Executive Order 13960

Executive Order 13960 on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government

https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government

FAR

Federal Acquisition Regulations

https://www.acquisition.gov/browse/index/far

FedRAMP

Federal Risk and Authorization Management Program

https://www.fedramp.gov/

FITARA

Federal Information Technology Acquisition Reform Act

https://www.congress.gov/bill/113th-congress/house-bill/1232

Final OMB AI Memo

Memorandum for Agency Use of AI

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

GAO

Government Accountability Office

https://www.gao.gov/

GSA

Government Services Administration

https://www.gsa.gov/

McCain NDAA

John S. McCain National Defense Authorization Act for Fiscal Year 2019

https://www.congress.gov/bill/115th-congress/house-bill/5515

NIST

National Institute of Standards and Technology

https://www.nist.gov/

Proposed OMB AI Memo

Proposed Memorandum for Agency Use of AI

https://ai.gov/wp-content/uploads/2023/11/AI-in-Government-Memo-Public-Comment.pdf

OMB

Office of Management and Budget

https://www.whitehouse.gov/omb/

2023 Racial Equity EO

Executive Order 14091 on Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government

https://www.whitehouse.gov/briefing-room/presidential-actions/2023/02/16/executive-order-on-further-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government/

VPAT

Voluntary Product Accessibility Template

https://www.section508.gov/sell/vpat/

cdt.org

cdt.org/contact

Center for Democracy & Technology
1401 K Street NW, Suite 200
Washington, D.C. 20005

202-637-9800

@CenDemTech

CENTER FOR
DEMOCRACY
& TECHNOLOGY