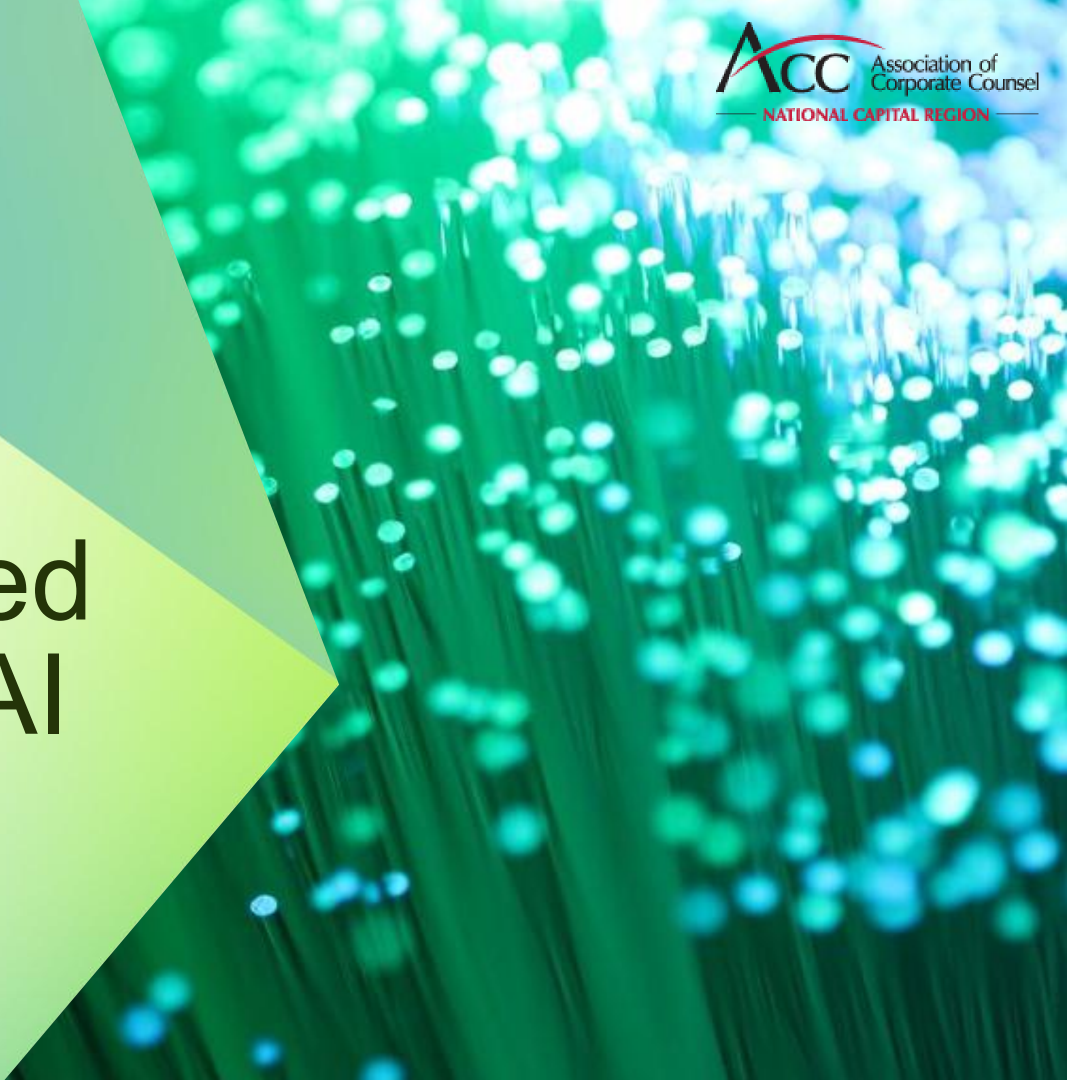
Hogan Lovells



ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

What All Government Contractors Need to Know About AI

Nathan Salminen, Hogan Lovells
Taylor Hillman, Hogan Lovells
Adriana Luedke, Lockheed Martin

July 30, 2025

Today’s Agenda

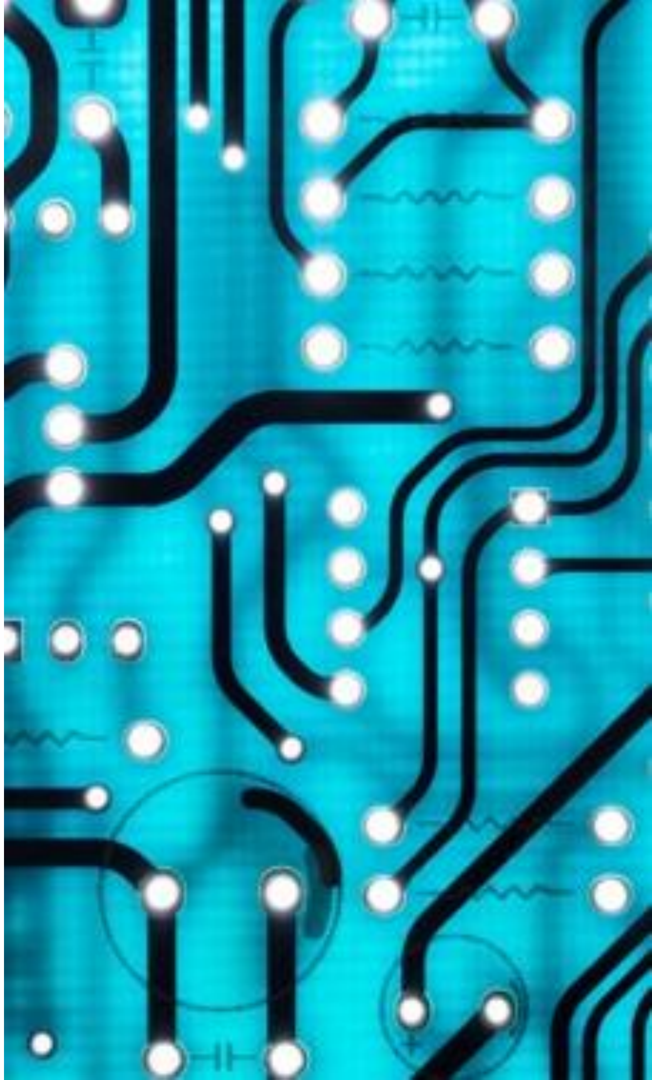
- Background
- Recent AI Regulatory Developments
- Implications for Government Contractors
- Government Procurement AI Regulatory History
- What Comes Next
- Other Government Policy towards AI in Acquisitions
- Questions

Background

Artificial Intelligence

The federal government predominantly adopts the definition of AI established in 15 U.S.C. § 9401, which characterizes AI as a machine-based system capable of making predictions, recommendations, or decisions that influence environments. This definition serves as a cornerstone for legislative, regulatory, and executive efforts related to AI. While variations exist in specific contexts, the core elements of this definition remain consistent across federal domains.

> The term “artificial intelligence” means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human based inputs to— (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action.



Different Types of AI

- Traditional/Regular
  - Analysis of existing data/rules to make predictions or classifications
  - Reactive
  - Examples: Computer playing chess; Google search algorithm; Netflix recommendation engine
- Generative
  - Creation of new content (*e.g.*, text, images, or code) based on learned patterns (*i.e.*, machine learning)
  - Proactive
  - Examples: Chatbots like ChatGPT; image generators like DALL-E; code generators like AlphaCode; content creation like Generative AI

AI use in Government

AI adoption has more than doubled during 2017 to 2022, according to a December 2022 McKinsey survey of 1,492 participants representing a range of regions, industries, and company sizes.

- "In 2017, 20 percent of respondents reported adopting AI in at least one business area, whereas today, that figure stands at 50 percent," the survey found.

The government is no exception

- Use cases of AI more than doubled from 710 in 2023 to 1,757 in 2024.
- AI applications are most common in administrative and IT functions, as well as health and medical areas.
  - Roughly 46% of AI use cases across the Federal government are categorized as mission-enabling, which includes management of finances, human resources, and facilities and properties. This also captures agency cybersecurity, IT, procurement, and other administrative functions.
- The Department of Health and Human Services (HHS), Department of Veterans Affairs (VA), Department of Homeland Security (DHS), and Department of the Interior (DOI) accounted for 50% of 2024's publicly-reported AI use cases.
- DOD Chief Digital and Artificial Intelligence Office (CDAO) announced award of four "Frontier-AI" contracts on July 14, 2025 to Anthropic, Google, OpenAI, and xAI – each with a $200M ceiling – intended "to accelerate DoD adoption of advanced AI capabilities to address critical national security challenges."

AI and Procurement

- Government use of AI in Government Procurement
  - Government agencies can use AI to create efficiencies, streamline acquisitions, and draft contracts.
  - Examples
    - GSA's Solicitation Review Tool (SRT) – reviews solicitations for Section 508 compliance
    - IRS' Contract Clause Review Tool – reviews contracts for missing or outdated clauses
- Government Purchase of AI
  - Increased opportunities for contractors to offer AI as part of their government offerings.
  - Creates unique risks for contractors – product liability, privacy, intellectual property, cyber, etc.
- Contractor use of AI in Government Contracts Performance
  - Contractor use of AI to create reports more quickly, track SOW requirements, review large data sets.
  - Risks include unsafeguarded public platforms and disclosure of proprietary/privileged information.

Recent AI Developments under Trump 2.0

Trump Administration Focal Points

- The Trump 2.0 Administration's new AI policies focus on innovation, agility, cost-effectiveness, and accountability to the tax-paying public.
- Prioritizing Made in America AI, and its aggressive stance towards China (the U.S.'s closest AI competitor) likely means that foreign AI systems, like Deep Seek, may face enhanced scrutiny if used by government contractors (foreign AI systems could even be barred for use by government agencies and contractors).
- Implementation and institution of Chief AI Officers (CAIOs) suggests the Trump Administration intends to widely install and utilize AI throughout the entirety of the executive branch.
- Two main AI OMB memos by the Trump Administration 2.0 (the AI Use Memo and AI Procurement Memo) place a heavy emphasis on the use of AI throughout the executive branch and federal workforce; they encourage the rapid and widespread adoption of AI by government agencies.
- The Trump Administration's past practices seem to indicate that many Biden Administration AI policies will be rescinded, revoked, replaced, or roll-backed in whole or in part.

Intact Biden Administration Developments

- Executive Order 14144: *Strengthening and Promoting Innovation in the Nation's Cybersecurity*
  - Calls for accelerating the development and deployment of AI to transform cyber-defense, in addition to focusing on the enhancement of cybersecurity across federal systems, supply chains, and critical infrastructure, particularly in response to persistent threats from adversarial nations such as China, Iran, Russia, and North Korea.
  - Calls for, by November 1, 2025, (i) the release of existing datasets for cyber defense research be made accessible to the broader academic research community, and (ii) the incorporation of management of AI software vulnerabilities and compromises into various agencies' existing processes and interagency coordination mechanisms for vulnerability management.
  - Revised significantly on June 6, 2025, by EO 14306: *Sustaining Efforts To Strengthen and Amending Executive Order 13694 and Executive Order 14144*. Maintained a focus on promoting cybersecurity with and in AI.

Executive Order 14179: *Removing Barriers to American Leadership in Artificial Intelligence* (Jan. 23, 2025)

- Calls for revision of OMB Memos (M-24-10 and M-24-18) issued under President Biden's Executive Order 14110 within 60 days to align with EO 14179.
- Requires AI Action Plan within 180 days of order to address policy objectives in EO 14179 (issued on July 23, 2025).
- Focuses on removing barriers to innovation and global AI dominance.
  - Advocates a policy of "sustain[ing] and enhanc[ing] America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security."

Memorandum M-25-21: *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*

- Known as the “OMB AI Use Memo.”
- This memorandum supersedes the previous M-24-10 and M-24-18 Memos issued by President Biden, marking a strategic shift in the federal government’s approach to AI.
- Emphasis on removing barriers to AI adoption, maintaining public trust, and mitigating risks.
  - Provides “guidance to agencies on how to innovate and promote the responsible adoption, use, and continued development of AI, while ensuring appropriate safeguards are in place to protect privacy, civil rights, and civil liberties, and to mitigate any unlawful discrimination.”
- Applies to “new and existing AI that is developed, used, or acquired by or on behalf of covered agencies.”
  - Does not apply to the Intelligence Community (CIA, NSA, FBI, DIA, etc.).
  - Does not cover AI when it is being used as a component of a National Security System.
  - The use and acquisition of AI in national security systems will be governed by guidance from the DoD.

Memorandum M-25-21: *OMB AI Use Memo*

Focus Areas:

- Removal of barriers to AI innovation
- Data and AI asset sharing
- Governance (including appointment of CAIOs)
- Transparency and accountability to the taxpayers
- Risk management for high-impact AI
  - High impact AI is AI "with an output that serves as a principal basis for decisions or actions with legal, material, binding, or significant effect" on civil rights, civil liberties, privacy, access to critical life opportunities or government services, human health and safety, critical infrastructure or public safety, or strategic assets or resources."
- Adopt policies to foster competition in AI procurement
- Maintaining a federal workforce trained in AI

- Implementation Timeline
  - □ Within 180 days and every 2 years after, agencies must post publicly the agency's plan to achieve the memorandum's goals or state that it does not intend to use AI
  - □ Within 270 days, agencies must (1) update internal IT infrastructure policies as needed to align with the memorandum, and (2) develop policies setting terms for acceptable use of generative AI, including safeguards and oversight to ensure it does not pose undue risk
  - □ All agencies except DOD and Intelligence Community must annually inventory AI use cases

Memorandum M-25-22: *Driving Efficient Acquisition of Artificial Intelligence in Government*

- Known as the "OMB AI Procurement Memo."
- Provides "guidance to agencies to improve their ability to acquire AI responsibly."
- Applies to "AI systems or services that are acquired by or on behalf of covered agencies" and includes "data systems, software, applications, tools, or utilities" that are "established primarily" for researching, developing, or implementing AI or where an "AI capability" is integrated into another process, operational activity, or technology system.
  - Does not apply to Intelligence Community agencies.
- Excludes AI that is "embedded" in "common commercial products" that are widely available for commercial use and have "substantial non-AI purposes or functionalities," along with AI "used incidentally by a contractor" during contract performance.

Memorandum M-25-22: *OMB AI Procurement Memo*

- Goals
  - Ensuring the Government and American public benefit from competitive American AI – market competition creates best value for taxpayer
  - Safeguarding taxpayer dollars by tracking AI performance and managing risk – AI systems must be fit for purpose and eviler results that preserve public trust
  - Promoting effective AI acquisition with cross-functional engagement – robust collaboration is key to addressing challenges and risks
- Focus Areas
  - Maximize use of American-made AI
  - Protect privacy rights
  - Protect Government rights, including IP
  - Encourage the use of modular, interoperable, and transparent AI solutions that can be rapidly deployed and scaled
  - Implement risk management policies to guide assessment of contract awards for AI services/systems

Memorandum M-25-22: *IP Considerations*

- Agencies need processes for addressing use of government data and to include appropriate contractual terms that delineate ownership and IP rights of the government and the contractor.
  - Careful consideration of respective IP licensing rights is even more important when an agency procures an AI system or service, including where agency information is used to train and develop the AI system.
- Emphasis on standardization across contracts where possible.
- Agencies should scope licensing and other IP rights to the intended use of AI to avoid vendor lock-in.
  - To avoid vendor lock-in – should be able to be easily reused without an agency, or another vendor, having to spend additional money to perform burdensome data conversions, build an entirely separate or redundant storage system, or otherwise duplicative work that is not a cost-effective use of taxpayer dollars.
  - Protections against lock-in include requirements for vendor knowledge transfers, data and model portability, providing agencies with rights to code/models produced in performance of a contract, and transparency in licensing and pricing.
- Ensuring components necessary to operate/monitor the AI system or service remain available for the acquiring agency to access and use for as long as necessary.
- Provide clear guidance on handling, access, and use of agency data/info to ensure that info must only be collected and retained by a vendor when reasonably necessary to serve the intended purposes of the contract.
- Ensuring contracts permanently prohibit the use of non-public inputted agency data and outputted results to further train publicly or commercially available AI algorithms absent explicit agency consent.

Executive Order: *Sustaining Select Efforts to Strengthen the Nation’s Cybersecurity and Amending Executive Order 13694 and Executive Order 14144* (June 6, 2025)

- Section 5 - Promoting Security with and in Artificial Intelligence.
  - Recognizing AI has the potential to transform cyber defense by rapidly identifying vulnerabilities, increasing the scale of threat detection techniques, and automating cyber defense.

- Requires by November 1, 2025, existing datasets for cyber defense research to be made accessible to the broader academic research community (either securely or publicly) to the maximum extent feasible, in consideration of business confidentiality and national security.

- Requires by November 1, 2025, DoD, DHS, and ODNI to incorporate the management of AI software vulnerabilities and compromises into their respective agencies’ existing processes and interagency coordination mechanisms for vulnerability management, including through incident tracking, response, and reporting, and by sharing indicators of compromise for AI systems.

Winning the Race: America’s AI Action Plan

- Released on July 23, 2025, with three accompanying executive orders.
- EO 14320: *Promoting the Export of the American AI Technology Stack*
  - Establishment of the American AI Exports Program.
  - Economic Diplomacy Action Group (EDAG) must coordinate mobilization of federal financing tools in support of priority AI export packages.
- EO 14318: *Accelerating Federal Permitting of Data Center Infrastructure*
  - Aims to facilitate the rapid and efficient buildout of AI data centers and infrastructure through use of federal lands and resources.
  - Encourages projects through financial support for specific types of projects, which could include loans, loan guarantees, grants, tax incentives, and offtake agreements.
  - Efficient and streamlined environmental reviews for AI data center projects.
  - Use of federal lands and identification of military installations for data center projects.
- EO 14319: *Preventing Woke AI in the Federal Government*
  - Truth-seeking - AI should be truthful, prioritize historical accuracy, scientific inquiry, and objectivity, and acknowledge uncertainty where it exists/reliable information is lacking.
  - Ideological Neutrality – AI should be neutral, nonpartisan, and not manipulate responses in favor of ideological dogmas.

AI Action Plan Pillars:

1) Accelerating AI Innovation

- Global dominance in AI
- Deregulation to allow private sector to develop AI without unnecessary hinderances and greater speed

2) Build American AI Infrastructure

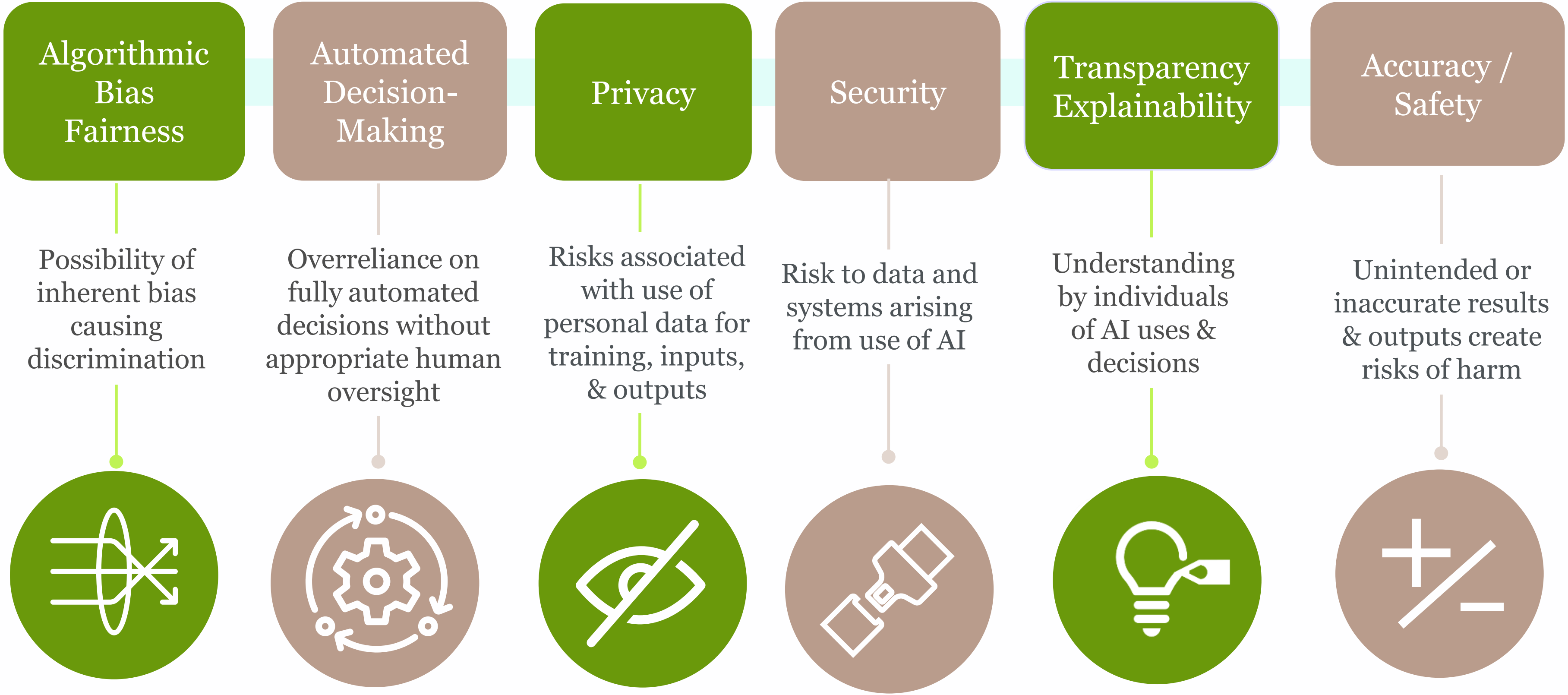
- Bolstering critical infrastructure cybersecurity
- Removing barriers to growing AI infrastructure

3) Lead in International AI Diplomacy and Security

- Driving adoption of American AI systems, computing hardware, and standards throughout the world through exports to allies, while preventing adversary access to American AI through export controls.

Implications for Government Contractors

Other Risks Associated with AI



Algorithmic Bias Fairness

Possibility of inherent bias causing discrimination

Automated Decision-Making

Overreliance on fully automated decisions without appropriate human oversight

Privacy

Risks associated with use of personal data for training, inputs, & outputs

Security

Risk to data and systems arising from use of AI

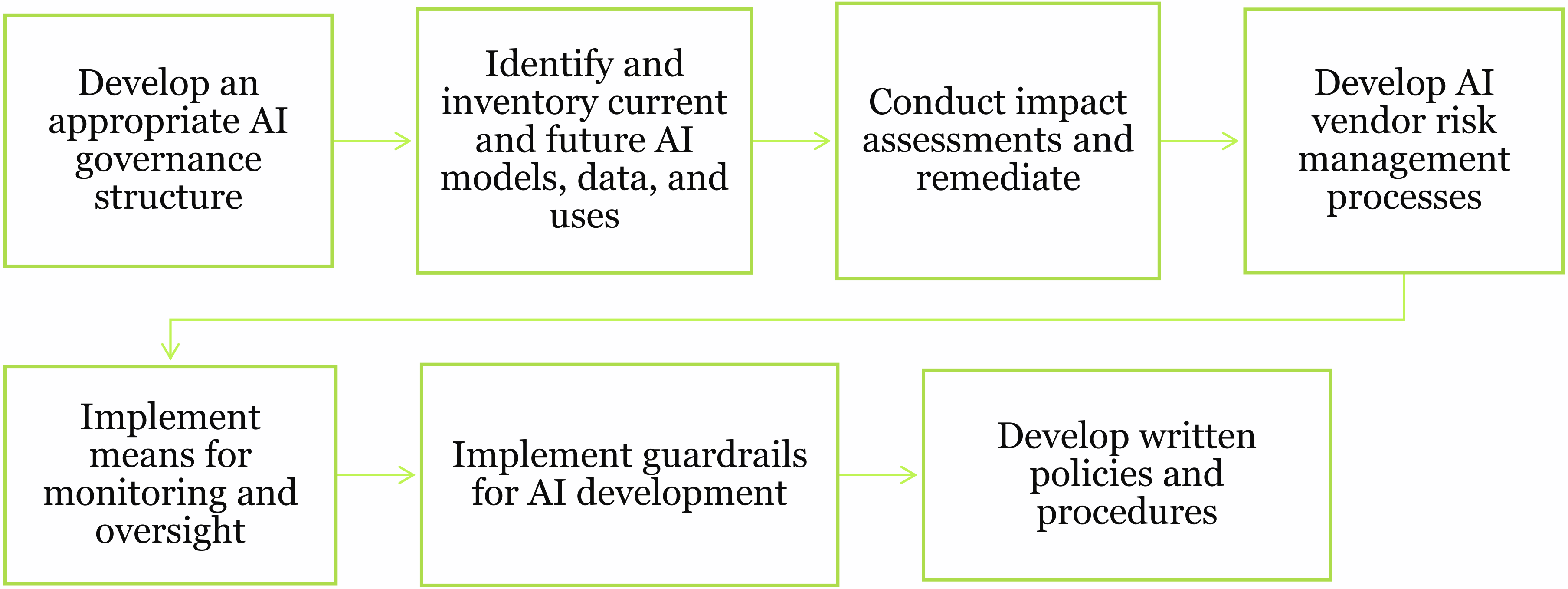
Transparency Explainability

Understanding by individuals of AI uses & decisions

Accuracy / Safety

Unintended or inaccurate results & outputs create risks of harm

Developing an AI Governance Program



Develop an appropriate AI governance structure

Identify and inventory current and future AI models, data, and uses

Conduct impact assessments and remediate

Develop AI vendor risk management processes

Implement means for monitoring and oversight

Implement guardrails for AI development

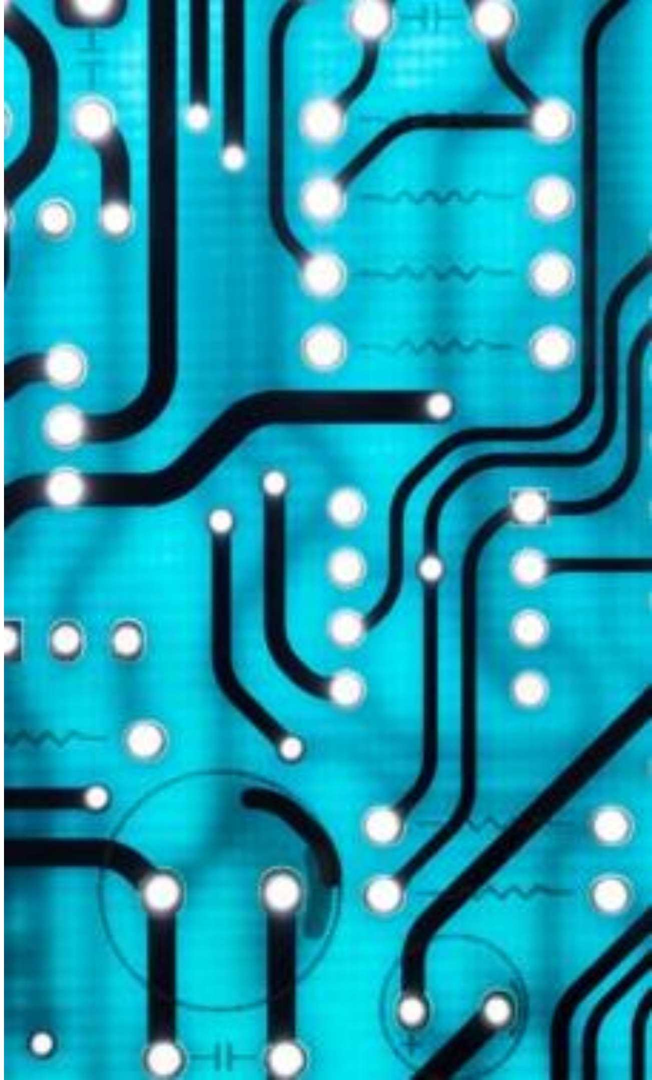
Develop written policies and procedures

Vendor Risk Management – Diligence

- The level of additional diligence for AI providers should reflect the level of risk.
- In many cases, the existing diligence process can be leveraged with additional factfinding.
- For cases where we are using the AI, additional questions might include:
  - Do the products and services incorporate AI?
  - What measures do you take with regard to bias, fairness, explainability and transparency?
- For cases where the vendor is training off or our data:
  - What customer data is used to train the AI?
  - Is that data identifiable?
  - What protections do you have in place to prevent the data from being exposed to third parties?

Vendor Risk Management – Contract Terms

- Many of the risks associated with AI can be addressed contractually.
- Examples include:
  - Prohibiting a vendor from using our data to train.
  - Failing that, placing restrictions around the use of our data for training.
  - AI-specific representations regarding transparency and explainability, in cases where that is relevant.
  - AI-specific cybersecurity terms in cases where the vendor is allowed to train with our data.
- A template set of terms is helpful.
- Note:
  - Legacy contracts often contain terms that allow the vendor to use customer data for purposes such as improving their services, which arguably would allow them to train AI with customer data. How might we identify those cases and impose AI terms where the level of risk justifies it?



Vendor Risk Management – Training Models

- It’s becoming increasingly common for AI and non-AI vendors to seek to use customer data to train AI.
  - One common scenario is that the major cloud providers now offer AI products that train off the contents of your tenant.
- Ways to mitigate risk:
  - Requiring the data be de-identified, both as to the individual and as to Tractor Supply.
  - Excluding business-sensitive data, such as intellectual property.
  - Seeking assurances from the developer regarding protections designed to keep the data from being exposed.
  - Only allowing the data to be used in a “fine tuning” context, where it trains only the version of the model used by Tractor Supply.

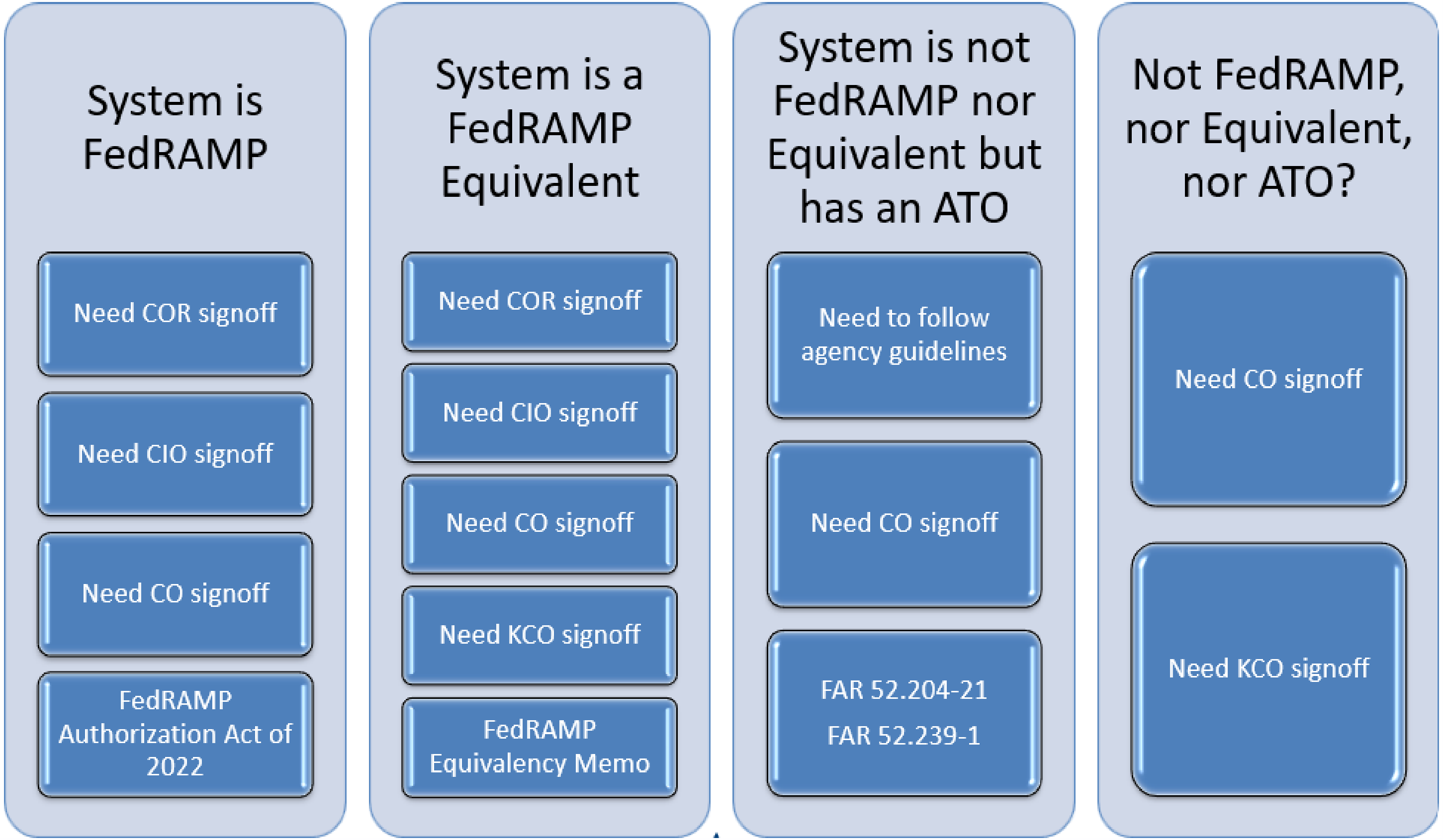
Contractor Considerations for use of AI

- Adoption of internal AI policies, including AI use policy, ethics, training of AI, building AI tools
  - Maintaining human oversight (possible input of IT experts with the technical AI knowledge, legal/compliance personnel)
  - DoD AI Code of Ethics
- Training on responsible AI usage (reliable, safe, secure, transparent, fair, bias-managed)
- Prioritize American-made AI systems
- Transparency in proposals when contemplating use of AI
- Seek Contracting Officer approval of AI usage in performance (sample language below)
  - As part of our performance under the above referenced contract Contractor has been asked by the Government to develop ________________. Contractor is proposing to use _____________ (include link to software/app), [a FedRAMP (authorized/equivalent) solution], that may involve the use of AI to execute this task.
  - The Government data that will be used includes the following:
  - We have discussed this approach with our COR (insert name), and (address any ground rules/rules of behavior that may have been provided by or discussed with the COR or any other Technical lead on the contract as applicable).

DoD AI Code of Ethics

- In February 2020, the DoD adopted a five-pillar framework for ethical AI following a comprehensive study by the Defense Innovation Board:
  - Responsible. DoD personnel will exercise appropriate levels of judgment and care, while remaining responsible for the development, deployment, and use of AI capabilities.
  - Equitable. The Department will take deliberate steps to minimize unintended bias in AI capabilities.
  - Traceable. The Department's AI capabilities will be developed and deployed such that relevant personnel possess an appropriate understanding of the technology, development processes, and operational methods applicable to AI capabilities, including with transparent and auditable methodologies, data sources, and design procedure and documentation.
  - Reliable. The Department's AI capabilities will have explicit, well-defined uses, and the safety, security, and effectiveness of such capabilities will be subject to testing and assurance within those defined uses across their entire life-cycles.
  - Governable. The Department will design and engineer AI capabilities to fulfill their intended functions while possessing the ability to detect and avoid unintended consequences, and the ability to disengage or deactivate deployed systems that demonstrate unintended behavior.

Contractor Considerations for use of AI



System is FedRAMP

- Need COR signoff
- Need CIO signoff
- Need CO signoff
- FedRAMP Authorization Act of 2022

System is a FedRAMP Equivalent

- Need COR signoff
- Need CIO signoff
- Need CO signoff
- Need KCO signoff
- FedRAMP Equivalency Memo

System is not FedRAMP nor Equivalent but has an ATO

- Need to follow agency guidelines
- Need CO signoff
- FAR 52.204-21
FAR 52.239-1

Not FedRAMP, nor Equivalent, nor ATO?

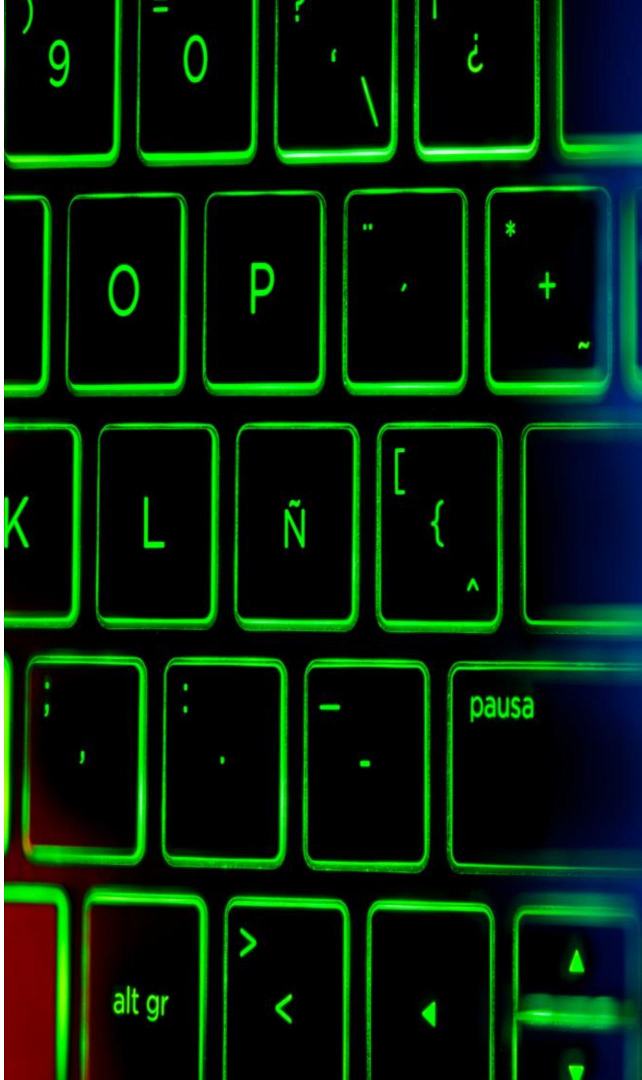
- Need CO signoff
- Need KCO signoff

Contractor Considerations for use of AI

- Review and negotiate IP and data rights clauses in AI contracts to protect interests and ensure compliance
  - Protection of AI outputs, risk allocation of bias/slippage/quality issues/etc.; copyright infringement; data protection and confidentiality; ensuring code is traceable to ensure limited govt rights can be applied; assessing whether contract data can be used to improve the contractor's AI
  - Tension between IP rights and push for COTS/commercial contracts
- Ensure incorporation of security and data protection controls when developing AI
- Use of AI applications that meet the NIST AI Risk Management Framework, FedRAMP and NIST SP 800-53 standards, or other safeguarding standards required by contract
- Evaluate solicitations to determine if they involve high-impact AI
  - This could necessitate additional compliance measures such as pre-deployment testing, AI impact assessments, continuous monitoring, and human monitoring
- Consider use of non-traditional procurement vehicles (Other Transaction Agreements) for sale of AI

Key Concerns and Considerations when Using AI

- Data trustworthiness
- Data governance
- Supply chain risk management
- Domestic preferences
- Cybersecurity
- Privacy
- Bias mitigation
- Intellectual Property
- Ethical use
- Human centered
- Testing
- Cross-Boarder Considerations



What Comes Next

What’s next?

- Trump may revoke or significantly revise the Biden Administration’s AI National Security Memorandum (“NSM”) to align it with President Trump’s AI policies.
- OMB will develop “playbooks” focused on the procurement of certain types of AI, including generative AI and AI-based biometrics. (AI Procurement Memo).
- OMB and GSA should release AI procurement guides for the federal acquisition workforce that will address “acquisition authorities, approaches, and vehicles.” (AI Procurement Memo)
- OMB and GSA will also likely release an online repository for agencies to share AI acquisition information and best practices, including language for standard AI contract clauses and negotiated costs. (AI Procurement Memo)
- The National Science Foundation and OSTP will draft and release a 2025 National AI R&D Strategic Plan.
- FAR/agency supplement clauses incorporating AI use and adoption goals

Government Procurement AI Regulatory History

Differences in Administration Focus on Contractors and AI

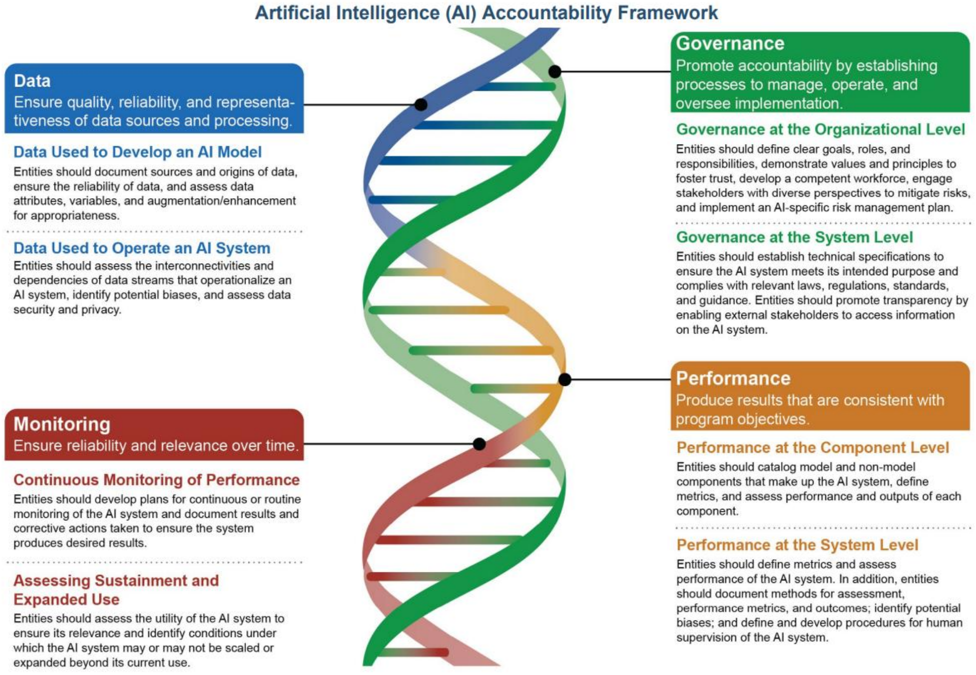
- Oversight vs. Deregulation:
  - The Biden Administration tended to focus on structured oversight and ethical considerations regarding AI, while the Trump Administration has tended to emphasize deregulation, innovation, and global dominance in AI.
- Equity & Civil Rights:
  - The Biden Administration emphasized principles of equity and civil rights protection throughout its AI EOs, OMB memos, and guidance, whereas the Trump Administration's recent policies focus on how bias generally (including DEI) can distort AI's effectiveness.
- Foreign Involvement in AI:
  - The Biden Administration aggressively regulated and licensed the export and foreign use of AI processing systems. The Trump Administration has taken a more open, flexible approach to allowing the export of AI to foreign countries, especially allies.

Trump Administration 1.0 Developments

- In response to the 2018 National Defense Strategy, which outlined various DoD objectives aimed at enhancing the U.S. military's competitive edge, including the use of and investment in AI, DoD issued a June 27, 2018 memorandum establishing the Joint Artificial Intelligence Center (JAIC).
  - Focused on the importance of AI in the future of society and war, with a goal of accelerating delivery of AI-enhanced capabilities.
- Executive Order 13859 (Feb 2019): *EO on Maintaining American Leadership in Artificial Intelligence*
  - Emphasized that the United States must maintain dominance in the development of AI through investment in research and development and a concerted Federal Government strategy called the American AI Initiative through the application of 5 key principles.
- Executive Order 13960 (Dec 2020): *EO on Promoting the Use of Trustworthy AI in the Federal Government*
  - Required the Federal Chief Information Officers Council (CIO Council) to establish "publicly available the criteria, format, and mechanisms for agency inventories of non-classified and non-sensitive use cases of AI by agencies."
  - Created nine "Principles for Use of AI in Government."
- Creation of the National Artificial Intelligence Initiative Office on January 12, 2021.

Agency Guidance under Biden Administration

- DoD Data, Analytics, and Artificial Intelligence Adoption Strategy
- DHS AI Task Force Guidance
  - DHS Policy Statement 139-06: Establishes foundational principles for AI acquisition and use within DHS, ensuring alignment with Executive Order 13960 and adherence to constitutional and legal standards.
- GAO Accountability Framework for Federal Agencies and Other Agencies (pictured right)
  - Published June 30, 2021
  - GAO's objective was to identify key practices to help ensure accountability and responsible AI use by federal agencies and other entities involved in the design, development, deployment, and continuous monitoring of AI systems.
  - Developed an AI accountability framework organized around four complementary principles: governance, data, performance, and monitoring.



Artificial Intelligence (AI) Accountability Framework

Data
Ensure quality, reliability, and representativeness of data sources and processing.

Data Used to Develop an AI Model
Entities should document sources and origins of data, ensure the reliability of data, and assess data attributes, variables, and augmentation/enhancement for appropriateness.

Data Used to Operate an AI System
Entities should assess the interconnectivities and dependencies of data streams that operationalize an AI system, identify potential biases, and assess data security and privacy.

Monitoring
Ensure reliability and relevance over time.

Continuous Monitoring of Performance
Entities should develop plans for continuous or routine monitoring of the AI system and document results and corrective actions taken to ensure the system produces desired results.

Assessing Sustainment and Expanded Use
Entities should assess the utility of the AI system to ensure its relevance and identify conditions under which the AI system may or may not be scaled or expanded beyond its current use.

Governance
Promote accountability by establishing processes to manage, operate, and oversee implementation.

Governance at the Organizational Level
Entities should define clear goals, roles, and responsibilities, demonstrate values and principles to foster trust, develop a competent workforce, engage stakeholders with diverse perspectives to mitigate risks, and implement an AI-specific risk management plan.

Governance at the System Level
Entities should establish technical specifications to ensure the AI system meets its intended purpose and complies with relevant laws, regulations, standards, and guidance. Entities should promote transparency by enabling external stakeholders to access information on the AI system.

Performance
Produce results that are consistent with program objectives.

Performance at the Component Level
Entities should catalog model and non-model components that make up the AI system, define metrics, and assess performance and outputs of each component.

Performance at the System Level
Entities should define metrics and assess performance of the AI system. In addition, entities should document methods for assessment, performance metrics, and outcomes; identify potential biases; and define and develop procedures for human supervision of the AI system.

Source: GAO. | GAO-21-519SP

Rescinded or Replaced Biden Administration Actions

- Executive Order 14110: *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (rescinded by EO 14179: *Removing Barriers to American Leadership in Artificial Intelligence*)
- Executive Order 14141: *Advancing United States Leadership in Artificial Intelligence Infrastructure* (rescinded by EO 14318)
- OMB AI Memos
  - Memorandum M 24-10: *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* (replaced via OMB Memo) - directed agencies to "advance AI governance and innovation while managing risks from the use of AI in the Federal Government, particularly those affecting the rights and safety of the public," name CAIOs, inventory AI use cases, eliminate barriers to responsible AI use, update FedRAMP, and adopt minimum risk policies for AI usage.
  - Memorandum M 24-18: *Advancing the Responsible Acquisition of Artificial Intelligence in Government* (replaced via OMB Memo) - directed agencies to improve their efficiency by responsibly acquiring AI.
- OFCCP Guidance for Federal Contractors (likely rescinded)
  - Directed federal contractors to promote effective enforcement and greater compliance with equal employment opportunity law when using AI for hiring.
- AI Diffusion Rule (rescinded by BIS)
  - Created a worldwide license requirement and revised the license review policies for ECCN relating to AI.

Other Government Policy towards AI in Acquisitions

Other Federal Government AI Developments for Government Contractors

- Fiscal Year 2025 National Defense Authorization Act
  - DoD will seek to cooperate with industry, international, and interagency partners to optimize its employment of AI in a variety of functions, including for workflow optimization.
  - Requires DoD to establish guidelines and principles for using AI.
- Protecting AI and Cloud Competition in Defense Act of 2025 (May 2025)
  - Proposed bill – meant to ensure that DoD's new contracts protect competition in the AI markets, instead of giving an unfair advantage to a few big players.
  - Focus on data protection.
- No uniform regulations
  - No open FAR or DFARS cases; no proposed rules.

Agency-specific AI Guidance for Government Contractors

- Not many agencies have adopted their own policies related to contractor use of AI
- Some examples:
  - DHS
    - DHS Generative AI Public Sector Playbook (Jan. 6, 2025)
    - DHS Directive 139-08, Artificial Intelligence Use and Acquisition (Jan. 15, 2025)
  - DoD
    - DoD Data, Analytics, and AI Adoption Strategy (2023)
    - Responsible AI Strategy and Implementation Pathway (2022)
    - Responsible AI Toolkit (2023)
  - GSA
    - Use of Artificial Intelligence (AI) at GSA (Directive 2185.1A CIO) (June 7, 2024)

Questions?

Hogan
Lovells

hoganlovells.com

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.