THE GOVERNMENT CONTRACTOR®

Information and Analysis on Legal Aspects of Procurement

MARCH 25, 2026 | VOLUME 68 | ISSUE 12

¶ 66 FEATURE COMMENT: Flag On The Field: Artificial Intelligence And The State Of Play In Federal Contracting

Unless one has undergone a digital and social detox for the past year, Artificial Intelligence (AI) is very much a cross-industry "hot topic" with little sign of cooling. Worldwide spending on AI is expected to exceed $2 trillion in 2026, an increase of 37 percent from the 2025 projections. See World Economic Forum, The AI-energy nexus Will Determine AI's Impact. We Must Account for It Better (Mar. 16, 2026, 7:18 PM) https://www.weforum.org/stories/2025/12/ai-energy-nexus-ai-future/. Organizations across a variety of industry sectors are either incorporating or actively considering how AI can fit within their operational processes to improve workflow, productivity, and reduce costs.

The Federal Government has similarly undertaken aggressive steps to leverage AI and improve its operational efficiencies. Section 2 of Executive Order (EO) 14179, "Removing Barriers to American Leadership in Artificial Intelligence," signaled AI as a priority for the current administration "to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security." Exec. Order No. 14179, 90 Fed. Reg. 37365 (Jan. 31, 2025). Agency adoption and use of AI include the Department of Homeland Security's use of data analytics for vehicle detection to track unusual patterns in border crossing, market research for acquisitions, and the National Aeronautics and Space Administration's testing of an AI-powered medical assistant that would help diagnose and treat astronauts in space. See Dep't of Homeland Sec., Vessel Detection (DHS-38), U.S. Customs and Border Protection AI Use Cases (Mar. 16, 2026, 7:09 PM), https://www.dhs.gov/ai/use-case-inventory/cbp; Dep't of Homeland Sec., Artificial Intelligence for Market Research Contract, https://www.dhs.gov/sites/default/files/2022-12/AI%20for%20MArket%20Research%20DHS-gov.pdf; Space.com, NASA and Google Test AI Medical Assistant for Astronaut Missions to the Moon and Mars (Mar. 16, 2026, 7:11 PM), https://www.space.com/technology/nasa-and-google-test-ai-medical-assistant-for-astronaut-missions-to-the-moon-and-mars. The General Services Administration also launched USAi, a sandbox that allows agencies to test, experiment, and evaluate AI models and systems for deployment. See USAi, https://www.usai.gov/ (last visited Mar. 16, 2026). The Department of Defense has similarly undertaken an aggressive position including issuing an AI Strategy earlier this year that identifies seven "Pace-Setting Projects" to demonstrate the rapid development and deployment of AI to support DOD. See Dep't of Def., War Department Launches AI Acceleration Strategy to Secure American Military AI Dominance (Mar. 16, 2026, 7:13 PM) https://www.war.gov/News/Re leases/Release/Article/4376420/war-department-launches-ai-acceleration-strategy-to-secure-american-military-ai/.

The Federal Government's accelerated adoption of AI presents a multitude of opportunities for businesses when considering that the Federal Government spent $833.83 billion in contracting last fiscal year, see Archisha Mehan, Federal Contract Awards in FY25: Spending Patterns Across Agencies and Industries, GovSpend (Mar. 16, 2026, 7:16 PM), https://govspend.com/blog/federal-contract-awards-in-fy25-spending-patterns-across-agencies-and-industries/. AI presents an attractive pathway for businesses to market and sell their AI solutions to the Federal Government. However, before playing in the federal AI space, it is important for industry to understand the rules governing the state of AI in the Federal Government. Failure to abide by these rules could result in self-imposed market entrance pains or, worse, loss of market opportunities.

Recent controversy surrounding AI developer Anthropic underscores how politically and commercially sensitive these issues have become. Allegations that certain Large Language Model (LLM) systems may embed ideological bias or policy safeguards have intensified scrutiny from policymakers and contributed to the administration's push for "unbiased AI" procurement requirements. While the debate continues to evolve, including the scope of the administration's requirement that AI systems be "unbiased," the episode serves as a reminder that companies looking to sell AI systems to the Federal Government must be prepared to demonstrate neutrality, transparency, and compliance with emerging federal standards and directives.

Rules of the Game: What's In-Bounds Versus Out-of-Bounds—To avoid an offsides penalty, AI developers need to understand the rules under which they are playing. While the current administration prioritizes speed and innovation, AI must still be developed in alignment with current AI policy directives. In particular, AI developers will need to examine their AI offerings to ensure their AI systems are developed in compliance with the Unbiased AI Principles espoused in EO 14319, "Preventing Woke AI in the Federal Government." Exec. Order No. 14319, 90 Fed. Reg. 35389 (Jul. 28, 2025). Section 3 of the EO directs agencies to only procure LLM AI systems that are developed in accordance with the EO's Unbiased AI Principles. An LLM AI system comports with the Order's Unbiased AI Principles when it is developed to be (1) truth-seeking, "prioritiz[ing] historical accuracy, scientific inquiry, and objectivity, and shall acknowledge uncertainty where reliable information is incomplete or contradictory;" and (2) ideologically neutral, where the LLM AI system's responses are not manipulated "in favor of ideological dogmas." Id. at 35389–390. The EO defines an LLM system at Section 2(c) to mean "a generative AI model trained on vast, diverse datasets that enable the model to generate natural-language responses to user prompts." Id. at 35389. Examples include Chatbots, auto-complete writing assistance functions, and translation tools.

The Unbiased AI Principles espoused in EO 14319 are not necessarily limited to LLM systems but are to be applied to non-LLM systems. Section 4(a)(iv) of the EO directs the Director of the Office of Management and Budget to develop guidance for agencies to apply the Unbiased AI Principles to both LLM systems and other non-LLM AI models and systems. See id. at 35390. OMB Memorandum M-26-04 similarly incorporates this charge in subsequent guidance, directing agencies to implement the Unbiased AI Principles in their AI system procurements by:

- Including terms in any solicitation or contract for an LLM AI system to address compliance with the Unbiased AI Principles;

- Modifying, to the extent practicable, existing LLM AI system contracts to require compliance with the Unbiased AI Principles with modifications occurring before the exercise of any option to extend the period of contract performance; and

- Updating agency-specific procurement policies by March 11, 2026, to ensure that compliance with the Unbiased AI Principles is baked into procurement procedures and developing a process "for agency users of LLMs to report outputs that violate the Unbiased AI Principles."

Off. of Mgmt. & Budget, Memorandum No. M-26-04, *Increasing Public Trust in Artificial Intelligence Through Unbiased AI Principles* (2025) at 3, Agency Actions. These approaches, where practicable, are to be applied to "other types of generative AI capabilities, such as tools that assist with image, voice, or multimodal generation." Id. at 7, Appendix A(2)(B). For industry, companies should be taking a hard look at their AI systems to ensure they are being developed and operate in a manner that comports with the EO's Unbiased AI Principles. Failure to develop AI systems in accordance with the Principles could result in ineligibility for contract award and loss of contract opportunities. Non-compliance during contract performance could expose a contractor to breach of contract terms and conditions and potential False Claims Act violations, particularly if federal users are reporting non-compliance in accordance with those processes developed by an agency in accordance with OMB M-26-04.

Time to Play: What's the Federal Government's AI Acquisition Strategy?—Industry should also be cognizant of the policies and strategies agencies are to leverage when procuring AI/ML systems. OMB Memoranda M-25-21, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust* and M-25-22, *Driving Efficient Acquisition of Artificial Intelligence in Government* provide a panoptic view of how agencies are expected to procure AI. See Off. of Mgmt. & Budget, Memorandum No. M-25-21, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust* (2025); Off. of Mgmt. & Budget, Memorandum No. M-25-22, *Driving Efficient Acquisition of Artificial Intelligence in Government* (2025). The following "strategies" OMB recommends agencies consider when procuring AI/ML systems are particularly noteworthy to AI developers:

- *Made in America AI*: Although barriers are to be removed to accelerate AI innovation and adoption, agencies are encouraged to "maximize the use of AI products and services that are developed and produced in the United States." See Off. of Mgmt. & Budget, Memorandum No. M-25-22, *Driving Efficient Acquisition of Artificial Intelligence in Government* (2025) at 5, § 3.c. While it remains to be seen how agencies apply this "Made in America" prerogative, the domestic development of AI systems may provide a competitive advantage during evaluations.

- *Prioritizing Data Rights*: When procuring AI systems and models, agencies "should take steps to ensure that their contracts retain sufficient rights to Federal Government data and retain any improvements to that data, including the continued design, development, testing, and operation of AI" and to prevent vendor lock-in. See id. at 5, § 3.3. Organizations need to carefully read the terms in the solicitation and resulting contract to ensure their intellectual property rights are preserved and to avoid the potential loss of what makes their AI system unique.

- *Performance-Based Acquisitions*: Agencies are strongly encouraged to use performance-based acquisition techniques to evaluate, assess, and hold contractors to the intended purpose of AI systems or services and to perform post-award monitoring. See id. at 8, § 4.b.iii. Contractors should expect to see and negotiate AI service level agreements defining and specifying terms such as AI system performance, system availability, system functionality and limitations, error rates, support response, and data usage to avoid differing understandings during contract performance.

Companies interested in doing business with DOD must similarly be aware of certain underlying policies governing DOD's acquisition and use of AI/ML systems. As a threshold matter, DOD's Memorandum on *Implementing Responsible Artificial Intelligence* highlights five AI Ethical Principles DOD has adopted for the design, development, deployment, and use of AI capabilities. See Dep't of Def., *Implementing Responsible Artificial Intelligence in the Department of Defense* (2021). These principles are:

1. *Responsible*: DOD personnel will exercise appropriate levels of judgment and care, while remaining responsible for the development, deployment, and use of AI capabilities.

2. *Equitable*: DOD will take deliberate steps to

minimize unintended bias in AI capabilities.

3. *Traceable*: DOD's AI capabilities will be developed and deployed such that relevant personnel possess an appropriate understanding of technology, development processes, and operational methods applicable to AI capabilities, including transparent and auditable methodologies, data sources, and design procedure and documentation.

4. *Reliable*: DOD'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 AI capabilities' entire life cycle.

5. *Governable*: DOD 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. See id. at 1.

More recent guidance further informs contractors as to what DOD expects from a "responsible AI system." In addition to identifying certain "Pace-Setting Projects" to accelerate AI innovation, development, and deployment within the Department, DOD's Jan. 9, 2026 AI Strategy clarifies that "Responsible AI" is to mean AI models that (1) do not incorporate ideological "tuning" that interferes with their ability to provide objectively truthful responses to user prompts and (2) are free from usage policy constraints that may limit lawful military applications. See Dep't of Def., *Artificial Intelligence Strategy for the Department of War* (2026) at 5. To ensure AI models used by DOD comply with the AI Strategy, and by extension, EO 14319, the Memorandum directs:

> The [Chief Digital and Artificial Intelligence Office ("CDAO")] to establish benchmarks for model objectivity as a primary procurement criterion within 90 days, … the Under Secretary of War for Acquisition and Sustainment to incorporate standard "any lawful use" language into any DoW contract through which AI services are procured within 180 days …[, and] direct[s] the CDAO to ensure all existing AI policy guidance at the Department aligns with the directives laid out in this memorandum.

Dep't of Def., *Artificial Intelligence Strategy for the Department of War* at 5 (2026).

Playing It Safe & Secure; Even When a Machine Is Doing the Thinking—As with any form of information technology, developing AI/ML systems requires active consideration of privacy and security. OMB guidance directs agencies to "establish policies and processes, including contractual terms and conditions, that ensure compliance with privacy requirements in law and policy whenever agencies acquire an AI system or service, or an agency contractor uses an AI system or service, that will create, collect, use, process, store, maintain, disseminate, disclose, or dispose of Federal information containing personally identifiable information (PII)." Off. of Mgmt. & Budget, Memorandum No. M-25-22, *Driving Efficient Acquisition of Artificial Intelligence in Government* (2025) at 5, § 3(d). For contractors this requires implementing and maintaining the necessary security controls to prevent unauthorized disclosure of or access to data that may be sensitive or constitute PII.

With respect to cybersecurity, AI is a double-edged sword because it has the capability to offer stronger and more advanced detection and cyber-threat response and mitigation measures. However, it also provides the capability to develop new, advanced attack vectors, including more sophisticated, AI-enabled adaptive malware that "learn" to become harder to identify, eradicate, or mitigate. To address these risks, the National Institute of Standards and Technology's (NIST's) AI Risk Management Framework and NIST Special Publication (SP) 800-218A highlight certain best practices organizations should implement when designing, developing, deploying, or using AI systems. See Nat'l Inst. of Standards & Tech., NIST AI 100-1, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (2023); Nat'l Inst. of Standards & Tech., SP 800-218A, *Secure Software Development Practices for Generative AI and Dual-Use Foundation Models: An SSDF Community Profile* (2024). These publications build upon existing NIST security and risk management frameworks, such as NIST's SP 800-218, which serves as a companion piece to NIST SP 800-218A, "by adding practices, tasks, recommendations, considerations, notes, and informative references that are specific to AI model development throughout the software development life cycle." Nat'l Inst. of Standards & Tech., SP 800-218A, *Secure Software Development Practices for Generative AI and Dual-Use Foundation Models* (2024) at i. For DOD-deployed AI systems, the Department's AI Cybersecurity Risk Management Tailoring Guide provides guidance on the acquisition, development, use, sustainment, and monitoring of any AI system used or operated by DOD (or on its behalf by a contractor), emphasizing confidentiality, integrity, and availability through the implementation of AI-tailored security controls that are built upon and mapped to DOD Instruction 8510.01, *Risk Management Framework for DOD Systems*. See Dep't of Def., *DOD Artificial Intelligence Cybersecurity Risk Management Tailoring Guide* (2025).

Contractors must also be cognizant of those safeguarding requirements specified in their solicitations and contracts. An AI system is ultimately a combination of hardware, software, and data, and as such, will most certainly require contractor compliance with certain safeguarding requirements under federal procurement regulation. At a minimum, contractors must ensure their AI systems comply with the 15 "controls" specified under Federal Acquisition Regulation 52.204-21. If developing an AI system under a DOD contract and where the system will process, store, and transmit covered defense information or controlled unclassified information, compliance with Defense FAR Supplement 252.204-7012 and the implementation of the Cybersecurity Maturity Model Certification (CMMC) Program at DFARS 252.204-7021 would most certainly also come to bear, requiring implementation of the 110 security controls specified under NIST SP 800-171 r2.

Looking forward, AI developers should also take stock of future cybersecurity requirements in development. In particular, Section 1513 in the recent National Defense Authorization Act for Fiscal Year 2026 directs DOD to develop an AI/ML physical/cybersecurity risk-based framework including (1) drawing upon existing cybersecurity reference documents, including the NIST SP 800 series and (2) implementing this "CMMC for AI/ML" as an extension or augmentation of existing DOD cybersecurity frameworks, including the CMMC Program. See Nat'l Def. Authorization Act for Fiscal Year 2026, P.L. 119-60, § 1513(a)(4), 139 Stat. 718, 1149 (codified at 10 USCA § 2224 note) (2025). While it remains to be seen how this AI/ML CMMC adjacent program will ultimately shape out and when it will be implemented, industry should pay close attention to whether new or additional text is added to security controls when an AI/ML system will process, transmit or store covered information. Knowing the rules and strategies, and planning for eventual contingencies, will better prepare those organizations actively considering opportunities to market and expand their AI offerings to the Federal Government.

♦

This Feature Comment was written for* T<span>HE</span> *G*OVERNMENT *C*ONTRACTOR *by* Philip Lee. *Mr. Lee is an Associate in the Government Contracts and Global Trade Group based in the Washington, D.C. office of McCarter & English. He can be reached at plee@mccarter.com.