JENNER & BLOCK

AI for GSA Contractors: Advanced Notice of MAS Refresh 31 Contains Significant Draft Changes, Deadline of March 20 for Comments

Client Alerts

March 12, 2026
By: David Robbins, Aaron R. Cooper, Moshe B. Broder, Elizabeth Pullin

The Administration's 2026 AI Action Plan foreshadowed broad efforts to bring Artificial Intelligence (AI) capabilities to government. Now, the General Services Administration (GSA), which leverages government-wide purchasing power, is proposing a new, required clause, GSAR 552.239-7001, Basic Safeguarding of Artificial Intelligence Systems, in all solicitations and contracts in which Artificial Intelligence (AI) capabilities are either (a) provided to the government or (b) used by the contractor as part of performance of the contract. The plain language of the draft clause also indicates that its compliance scheme applies to contractors doing business with GSA and also commercial AI service providers supporting GSA contractors.

GSA published the draft clause on March 6, 2026, as part of the advance notice for Multiple Award Schedule (MAS) Solicitation Refresh 31 (Solicitation No. 47QSMD20R0001), at buy.gsa.gov. GSA now seeks public and industry comment on the proposed new clause by March 20, 2026, meaning that time is of the essence for those seeking to share their views with the government. GSA also requires contractor acceptance of the mass modification no later than 60 days after the modification has been issued.

As government contractors evaluate the draft clause and consider whether to submit comments, they should assess several key features.

The draft clause would impose a variety of new and potentially significant obligations on government contractors and AI service providers in the government contracting space alike. In particular, the draft clause:

- places responsibility for AI use in the performance of GSA contracts squarely with prime contractors;
- requires that AI systems used for GSA contracts be produced and developed in the United States;
- retains for the government ownership of government data and certain AI developments;

- prohibits a broad range of data uses by contractors and service providers;
- establishes robust compliance, documentation, and reporting requirements; and
- subjects contractors to unannounced government assessments of their AI systems for bias and ideological neutrality.

In anticipation of some or all of the proposed clause taking effect, government contractors should immediately consider compliance and risk assessments–along with appropriate additional action–even if they do not formally "provide" AI capabilities to the government and only use AI in furtherance of other contract performance.

The prescribing language states that the draft clause must be inserted in "solicitations and contracts for Artificial Intelligence capabilities"—i.e., those contracts whose purpose is to provide AI capabilities to the government. But the text of the clause could imply a broader application, specifying that a contractor is responsible for service provider compliance not only where it provides an AI System but also where it uses an AI system as part of performance of the contract. Further, the proposed clause would require contractors to "disclose all AI systems used in performance of the contract . . . and whether the AI system has been modified or configured to comply with any non-US federal government or commercial compliance or regulatory framework . . .."

As a warning to entities using AI-as-a-service, the draft GSA clause states that it controls in the event of any conflict between the clause and the service provider's commercial terms and conditions.

Potential Scope

Although the clause, by its terms, applies to GSA's "prime contractors," it will have significant implications for all AI "Service Providers." As defined, an AI "Service Provider" is "an entity that directly or indirectly provides, operates, or licenses an AI system but is not a party to the contract. Service Providers may or may not be subcontractors." 552.239-7001(a).

The clause adopts a prior statutory definition of "AI System" as "any data system, software, application, tool, or utility that operates in whole or in part using dynamic or static machine learning algorithms or other forms of artificial intelligence, including systems developed for research and development of AI generally and systems where an AI capability is integrated into another agency business process, operational activity, or technology system." The definition does not include any "common commercial product within which AI is embedded, such as a word processor or map navigation system." *Id.*

American AI Systems are those "developed and produced" in the United States.[1]

Responsibility for Subcontractors and Service Providers

The clause makes clear that prime contractors performing under GSA contracts would be responsible for ensuring their service providers comply with the clause—even where the AI is owned and operated by a third-party platform provider not party to the contract. The OMB memorandum provides a two-part test for analyzing whether an AI product or service is excluded from the definition of a covered AI system: (1) whether the product or service is widely available to the public for commercial use, as opposed to being specialized or customized for governmental use; and (2) whether the AI is embedded in a product that has substantial non-AI purposes or functionality. OMB Memorandum M-25-22 at 3.

Contractors that rely on commercial AI platforms, cloud-based AI services, or subcontractor-provided AI tools should review their existing agreements with those providers now, as conflicts between commercial terms of service and this clause—which the clause resolves in the government's favor—are likely.

American AI Required

The clause would require GSA contractors to use AI produced or developed in America. "The use of foreign AI systems in the performance of GSA contracts, including any AI components manufactured, developed, or controlled by non-US entities is prohibited." 552.239-7001(e)(2). This requirement extends to all components of the AI system, and contractors whose solutions incorporate elements from non-US developers—including foreign-origin open-source model components—will need to carefully assess their AI supply chains.

Government Ownership of Data and Custom Developments

Section (d) of the clause establishes the government's broad and immediate ownership rights over two categories of information generated under the contract.

a. Government Data is defined to include all data inputs—such as user prompts, queries, instructions, system prompts, source documents, and knowledge bases submitted to the AI system—as well as all data outputs generated by the AI system, including responses, analyses, logs, metadata, and synthetic data. 552.239-7001(a).

b. Custom Developments include any modifications, configurations, fine-tuning, enhancements, or training results developed specifically for the government under the contract. Notably, this definition captures the results of model fine-tuning or training performed on government data—meaning that a customized or fine-tuned model developed under the contract belongs to the government, not the contractor. 552.239-7001(d)(5).

Under the draft clause, contractors and service providers would receive only a limited, revocable, non-exclusive license to use government data and custom developments for the duration of the contract and solely for permitted contract performance purposes. Any intellectual property rights that a contractor or service provider acquires in government data would then be immediately assigned to the government upon creation. Contractors retain ownership of their underlying base models only. 552.239-7001(d)(1).

Prohibited Uses of Government Data

The clause enumerates specific prohibited uses of government data by contractors and service providers. These prohibitions apply regardless of the commercial practices or policies of any AI platform used in performance. Prohibited uses include:

- **Training or improving AI models.** Contractors and service providers may not use government data to train, fine-tune, or otherwise improve any large language model or other AI or machine learning model—including models operated by third parties—for any commercial or non-commercial purpose.
- **Informing business operations.** Government data may not be used to target government or non-government entities or to inform the contractor's or service provider's advertising, marketing, sales, monetization, strategy, or other business decisions.
- **Unauthorized retention.** Contractors may not retain, access, or use government data beyond the scope and duration expressly permitted in the contract. 552.239-7001(d)(3).

Data Handling, Segregation, and Secure Deletion

The draft clause imposes detailed data handling obligations beyond general security requirements. Contractors and service providers must implement "eyes off" data handling procedures restricting human review of government data to what is strictly necessary, with all human access logged, justified, and made visible to the government. 552.239-7001(d)(4)(ii).

Government data must be logically segregated from the data of any non-government customers, with defense-in-depth protections including access controls, encryption, and continuous monitoring

against unauthorized access. *Id.* at (v).

Data localization requirements prohibit transmission or storage of government data outside of agreed-upon premises or authorized services without express written consent from the ordering agency. *Id.* at (iv).

Compliance, Reporting, and Documentation

For all AI products used in contract performance, GSA contractors would be required to disclose to the ordering Contracting Officer all AI systems used and whether any AI system has been modified or configured to comply with any non-US federal government or commercial compliance or regulatory framework, within 30 days of contract award or earlier if requested. 552.239-7001(e)(1).

The clause requires contractors to provide the government with the means to implement human oversight, intervention, and traceability. For AI systems using intermediary processing—such as reasoning, retrieval-augmented generation (RAG), or agentic processes—the system must summarize intermediate steps from data input to output and make that information accessible through data output, audit trail, and user interface. At minimum, the AI system must include: (1) summarized intermediate processing actions and decision points; (2) model routing decisions with accompanying rationale; and (3) data retrieval methods employed, including complete source attribution with direct links to source materials. 552.239-7001(e)(3).

Contractors must report cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) and the Contracting Officer within 72 hours of detecting a confirmed or suspected incident, with daily status updates until resolution. Relevant logs, forensic artifacts, and images must be preserved for a minimum of 90 calendar days to facilitate law enforcement investigation. Where these reporting requirements conflict with FedRAMP incident communication and response procedures, FedRAMP procedures control. 552.239-7001(e)(4).

The compliance scheme also would require contractors to provide documentation sufficient to demonstrate compliance, including AI system decision-making processes, logic, and operational parameters; documentation consistent with the NIST AI Risk Management Framework, including system cards or equivalent materials; privacy control effectiveness and PII processing prohibitions; testing methodologies for detecting and mitigating bias; documentation of known biases and limitations; and any other documentation necessary for the government to complete an AI Impact Assessment required by OMB M-25-21. 552.239-7001(e)(6).

As to privacy protection, the clause would require contractors and service providers, to the extent they have available tools, to provide the government with configurable controls to manage, prevent, and reject the entry or persistence of PII within the AI system. 552.239-7001(f).

Unbiased AI Principles and Government Evaluation Rights

Section (i) of the clause establishes a framework for AI performance and ideological neutrality that is both novel and consequential. Contractors must use commercial efforts to ensure that AI systems are truthful in responding to factual queries—prioritizing historical accuracy, scientific inquiry, and objectivity—and operate as neutral, nonpartisan tools that do not manipulate responses in favor of ideological positions. The clause specifically identifies "Diversity, Equity, Inclusion" as an example of prohibited ideological dogma. Contractors may not intentionally encode partisan or ideological judgments into AI system outputs. 552.239-7001(i)(1).

Reinforcing the ideological neutrality requirement, the clause also prohibits AI systems from refusing to produce outputs or conduct analyses based on the contractor's or service provider's discretionary policies. 552.239-7001(d)(2)(ii). In practical terms, this would mean that an AI platform's standard commercial content moderation policies, built-in safety guardrails, or default refusal behaviors cannot be used to decline a government request under the contract. The clause clarifies that this obligation would not require retraining the model or altering model weights, but contractors should assess whether their AI service provider's default content policies are compatible with unrestricted government use—and if not, whether a configurable enterprise deployment can bridge that gap.

The government reserves the right to conduct unannounced automated assessments of the AI system at any time—as deployed and configured for government users—using its own benchmarks to evaluate bias, truthfulness, safety, and ideological content. Contractors would be required to provide tools and interfaces enabling the government to run these benchmarks against the production system. The government is under no obligation to disclose its benchmarks, test data, or methodologies to the contractor. 552.239-7001(i)(2).

If the contractor fails to comply with the Unbiased AI Principles and the government terminates the contract for cause as a result, the contractor may be liable for reasonable decommissioning costs. 552.239-7001(i)(3).

This section has significant practical implications for contractors whose AI service providers have built-in content moderation or safety policies that may not align with these requirements. Contractors should understand how their AI systems respond to politically and socially sensitive queries and engage their AI service providers on the implications of these obligations.

Data Portability

Consistent with OMB Memorandum M-25-22, the proposed clause requires data outputs to be open and interoperable. Contractors would be required to use open and standard data formats and APIs for all data outputs and AI systems and must avoid proprietary technologies or formats that create vendor dependencies or require additional licensing. Contractors must also provide tools enabling government customers to export all government data—including conversational history, uploaded documents, and custom knowledge bases—in open, machine-readable formats such as JSON or XML, preserving full structural and relational integrity. 552.239-7001(g).

Change Management

The clause imposes specific advance notice obligations for changes to AI systems during contract performance. Contractors would be required to provide the government 30 calendar days' notice before any planned material change to AI system disclosure requirements, before adding a new service provider, or before materially changing an existing service provider. 552.239-7001(h)(3), (4). If an AI service change materially increases output bias or decreases safety guardrails, the contractor must notify the government within 7 calendar days of identifying the change. *Id.* at (2). For model transitions, contractors would be required to provide access to successor models for a minimum 30-day evaluation period (15 days for minor versions) before discontinuing existing models. *Id.* at (1).

Conclusion

Jenner & Block lawyers are providing this update for interested companies. With our deep bench of experienced professionals, including leading advisors on AI and Government Contracts, we bring practical insights to guide clients in shaping the future regulatory and compliance scheme for doing business with the government. Companies wishing to submit comments on the draft rule, or to begin compliance and risk assessments should reach out to the authors or their usual Jenner & Block points of contact for assistance.

Footnotes

[1] *See* OMB Memorandum M-25-22, *Driving Efficient Acquisition of Artificial Intelligence in Government* (April 3, 2025).

Related Attorneys

David Robbins

Partner
drobbins@jenner.com
+1 202 639 6040

Aaron R. Cooper

Partner
acooper@jenner.com
+1 202 637 6333

Moshe B. Broder

Partner
mbroder@jenner.com
+1 202 637 6334

Elizabeth Pullin

Special Counsel
epullin@jenner.com
+1 202 639 3893

Related Capabilities

Critical and Emerging Technologies

Government Contractor Litigation and Compliance

© 2026 Jenner & Block LLP. Attorney Advertising. Jenner & Block LLP is an Illinois Limited Liability Partnership including professional corporations. This publication, presentation, or event is not intended to provide legal advice but to provide information on legal matters and/or firm news of interest to our clients and colleagues. Readers or attendees should seek specific legal advice before taking any action with respect to matters mentioned in this publication or at this event. The attorney responsible for this communication is Brent E. Kidwell, Jenner & Block LLP, 353 N. Clark Street, Chicago, IL 60654-3456. Prior results do not guarantee a similar outcome. Jenner & Block London LLP, an affiliate of Jenner & Block LLP, is a limited liability partnership established under the laws of the State of Delaware, USA and is authorised and regulated by the Solicitors Regulation Authority with SRA number 615729. Information regarding the data we collect and the rights you have over your data can be found in our Privacy Notice. For further inquiries, please contact dataprotection@jenner.com.

Stay Informed →