



PROGRAM MATERIALS
Program #36125
September 28, 2026

Artificial Intelligence in Federal Contracting: Risks, Obligations, and Opportunities

Copyright ©2026 by

- **Wojciech Kornacki, Esq. - Watson and Associates LLC**

All Rights Reserved.
Licensed to Celesq®, Inc.

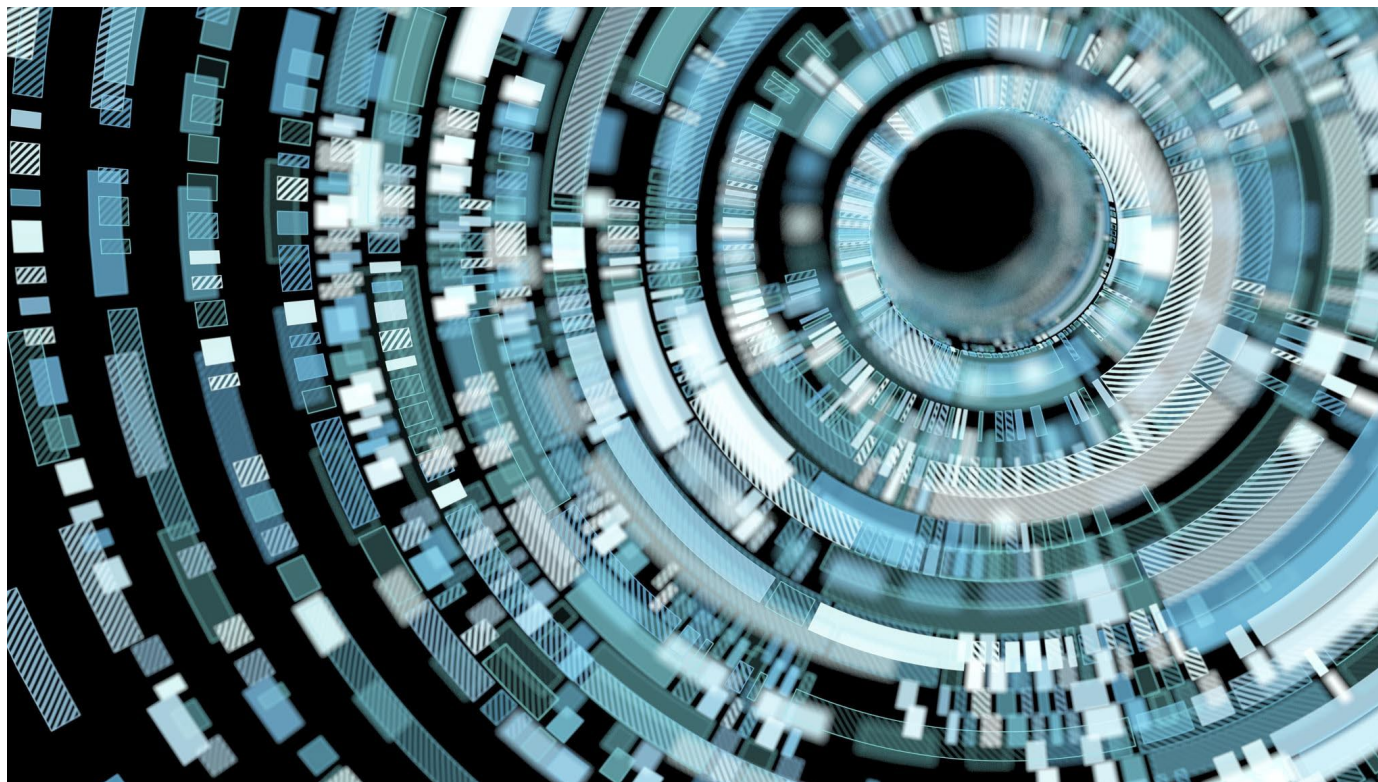
Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919



**Watson &
Associates, LLC**
Attorneys | Consultants

Artificial Intelligence In Federal Contracting



September 28, 2026
By Wojciech Z. Kornacki, Esq.

Lecturer

Not Legal Advice / For Educational Purposes Only

Agenda

- What are legal and compliance obligations for federal contractors using AI?
- What are the latest AI trends and developments in the federal contracting industry?
- What are the most recent enforcement actions by the U.S. Government against contractors using AI?

Sources

AI in Government Act (2020)

The Advancing American AI Act (2023)

NIST AI 300-1, Policy Framework – Artificial Intelligence (2026)

<https://www.nist.gov/artificial-intelligence>

Executive Order 14365 (2025)

Executive Order 13960 (2020)

OMB Memorandum, M-25-22, Driving Efficient Acquisition of AI in Government (2025)

NIST's AI Standards "Zero Drafts" (2026)

GSAR Clause 552.239-7001 (2026)



AI is a

system that performs tasks

system that solves tasks requiring **human-like skills**

system designed to think and act **like a human**

a set of techniques designed to approximate a **cognitive task**

a system designed to **act rationally** that achieves goals, plans, learns, reasons, and acts

intelligence for use within the Department.

(g) **ARTIFICIAL INTELLIGENCE DEFINED.**—In this section, the term “artificial intelligence” includes the following:

(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.



AI Revolution

**2000s
Mobile/Social
Medial Revolution
starts**

**2012s
AI Revolution
starts**



**1970s
Internet Revolution
starts**

**2000s
Internet
Revolution ends**

AI in Government Act (2020)

The AI Center of Excellence within the General Services Administration

The Office of Management and Budget (OMB) to issue a memorandum informing federal agencies of policies for acquisition and application of AI and identifying best practices for mitigating risks.

<https://coe.gsa.gov/coe/artificial-intelligence.html>



AI Capability Maturity Model

Organizational Maturity
Capacity to Execute and Manage
AI Initiatives.

Levels

- OPTIMIZED **5** ENTERPRISE
- MANAGED **4** PORTFOLIO
- DEFINED **3** PROGRAM
- REPEATABLE **2** TEAM PROJECT
- AD HOC **1** INDIVIDUAL PROJECT



coe.gsa.gov

The Advancing American AI Act (2023)

Take steps to promote AI while aligning US values (privacy, civil rights, civil liberties)

Consider AI risks and AI-enabled systems

National Policy Framework for AI

Federal permitting for AI infrastructure construction and cooperation

Develop technical capacity to understand frontier AI model capabilities

Provide grants, tax incentives and assistance programs to support wider AI deployment

Eliminate innovation barriers to allow the US lead the world in AI

Federal priority over states

Executive Order 14365

Sustain and enhance global AI dominance

DOJ AI Litigation Task Force

States will not impose restrictions conflicting with federal AI procurement and use of AI

Artificial Intelligence Ethics Framework for the Intelligence Community
(July 23, 2020)

Executive Order 14365

US Government AI Principles

- 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
- Accountable

Driving Efficient Acquisition of AI in Government

Focus on full and open competition

Improve Government efficiency and effectiveness



NIST - AI Standards “Zero Draft”

AI datasets and models for transparency between AI stakeholders

Documentation artifact (data element) – record describing a product or service, or portion thereof

It may take many forms, physical, or digital publication

AI system – engineered system that generates outputs, forecasts, recommendations, or decisions

AI model – architecture and parameters, it does not include components



GSAR Clause 552.239-7001 (pending review)

~~Intelligence for the Department.~~

(g) ARTIFICIAL INTELLIGENCE DEFINED.—In this section, the term “artificial intelligence” includes the following:

(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.



GSAR Clause 552.239-7001 (pending review)

(c) *Contractor Responsibility for Service Provider AI.* If the Contractor is providing or using as part of performance of this contract an AI System owned and/or operated by a Service Provider then the Contractor is responsible for the Service Provider's adherence to this clause.

(2) *License Grant to Government.* The Contractor grants to the Government an irrevocable, royalty-free, non-exclusive license to use the AI System for the duration of this contract for any lawful Government purpose. This license includes the right to:

- (i) Operate and access the AI System through agreed-upon methods;
- (ii) Input Data Inputs and receive Data Outputs. The AI System must not refuse to produce data outputs or conduct analyses based on the Contractor's or Service Provider's discretionary policies. This requirement must not be construed to require retraining of the model or alteration of model weights;



GSAR Clause 552.239-7001 (pending review)

(i) The Contractor and Service Provider must implement reasonable technical, administrative, physical, and organizational safeguards to protect Government Data from loss, damage, destruction, unauthorized alteration, or corruption, and prevent its unauthorized, accidental, or unlawful access, disclosure, use, or processing.

(3) *Prohibited Uses of Government Data.* Examples of prohibited use of Government Data includes:

(i) Training, fine-tuning, or otherwise improving an LLM or other machine learning or AI models, including those operated by third parties, or to develop or improve the AI System(s) for any other customers or any commercial or non-commercial purposes.

(ii) Targeting Government or non-Government entities or informing Contractor's or Vendor's advertising, marketing, sales, monetization, strategy, operations or other business decisions.

(iii) Retaining, accessing, or using beyond the scope and duration expressly permitted in the contract.



GSAR Clause 552.239-7001 (pending review)

(e) *Contractor Obligations for Compliance, Reporting, and Documentation.* The Contractor must:

(1) The contractor must disclose all AI systems used in performance of this contract to the ordering contracting officer, and whether the AI system has been modified or configured to comply with any non-U.S. federal government or commercial compliance or regulatory framework no later than thirty (30) days after award, unless requested earlier by the ordering contracting officer.

(2) *American AI Systems.* The Contractor and Service Provider must use only American AI Systems. The use of foreign AI systems in the performance of this contract, including any AI components manufactured, developed, or controlled by non-U.S. entities, is prohibited.

(3) *Human Oversight.* Provide a means for the Government to implement human oversight, intervention, and traceability. If the AI system uses intermediary processing such as reasoning, retrieval, or agentic processes, the AI system must summarize intermediary steps from data input to data output, and make this information accessible through data output, audit trail, and as applicable the user interface. At minimum, the AI system must include:

- (i) Summarized intermediate processing actions and decision points;
- (ii) Model routing decisions with accompanying rationale; and
- (iii) Data retrieval methods employed (e.g., Retrieval-Augmented Generation (RAG), web search), including complete source attribution including direct links and relevant excerpts from materials used in response generation.



GSAR Clause 552.239-7001 (pending review)

(4) *Incident Reporting.* The Contractor or Service Provider must complete the CISA incident reporting form (<https://myservices.cisa.gov/irf>) and notify the Contracting Officer and any Government provided point of contacts as soon as possible but not longer than within 72 hours of the discovery of any confirmed or suspected incident (as defined by the Federal Information Security Modernization Act of 2014 in 44 U.S.C. § 3552(b)(2)) and provide daily status updates to all points of contact until resolved.

(i) Such notification must include, to the extent known at the time:

- (A) Nature and scope of the incident;
- (B) Data potentially affected;
- (C) Immediate remediation steps taken;
- (D) Timeline for full resolution; and
- (E) Measures to prevent recurrence

(ii) Where FedRAMP incident communication and response procedures conflict with contractual requirements, the FedRAMP procedures must apply.

GSAR Clause 552.239-7001 (pending review)

- (5) *Feedback Reporting.* The Contractor must establish feedback mechanisms allowing the Government to:
- (i) Provide performance feedback and improvement requests through formal channels;
 - (ii) Request system modifications or enhancements; and
 - (iii) Report operational concerns without requiring incident classification.

GSAR Clause 552.239-7001 (pending review)

- (5) *Feedback Reporting.* The Contractor must establish feedback mechanisms allowing the Government to:
- (i) Provide performance feedback and improvement requests through formal channels;
 - (ii) Request system modifications or enhancements; and
 - (iii) Report operational concerns without requiring incident classification.



GSAR Clause 552.239-7001 (pending review)

(6) *Documentation.*

(i) Provide, upon Government request, and under appropriate confidentiality protections, existing commercial documentation or disclosures sufficient to demonstrate compliance, including but not limited to:

(A) Verification of compliance with this clause and the contract;

(B) AI System decision-making processes, logic, and operational parameters;

(C) System documentation consistent with NIST AI Risk Management Framework guidelines, Unbiased AI Principles, and LLM Transparency requirements such as system cards or equivalent documentation;

(D) Privacy controls effectiveness and PII processing prohibition compliance;

(E) Testing methodologies used to detect and mitigate noncompliance with the unbiased AI principles described in paragraph (i)(1);

(F) Known biases (including commercial, political, or personal considerations, advertising, endorsements, or fraudulent/corrupt interests), limitations, truthfulness concerns, and performance metrics; and

(G) Any other information necessary for the Government to monitor and evaluate the AI system's performance, risks, and effectiveness and to complete an AI Impact Assessment required by OMB M-25-21.

(ii) Confidential documentation and information provided by the Contractor must not be disclosed by the Government absent specific legal requirements.



GSAR Clause 552.239-7001 (pending review)

(f) *Privacy and Confidentiality Protections.* To the extent the Contractor or Service Provider has available tools, they must provide tools to enable the Government to implement appropriate Government-configurable controls, including but not limited to automated detection mechanisms and clear user notifications to manage, prevent, and reject the entry or persistence of PII within the AI System.



GSAR Clause 552.239-7001 (pending review)

(2) The Contractor must notify the Government within seven (7) calendar days of identifying any AI service change that materially increases output bias or decreases safety guardrails or behavioral constraints impacting lawful usage or the performance or truthfulness of outputs. The notification must describe the change, its purpose, the evaluation approach used and any new limitations, trade-offs, or potential negative impacts identified.



GSAR Clause 552.239-7001 (pending review)

(2) Government Evaluation Rights and Remediation.

(i) The Government reserves the right to conduct automated assessments of the AI system, as deployed and configured for government users, at any time using its own benchmarks. These evaluations may assess bias, truthfulness, safety, unsolicited ideological content, and other factors determined by the Government in order to facilitate evaluations.

(ii) The Contractor must provide tools and interfaces that enable the Government to run its benchmarks in an automated fashion to test the production AI system and identify any material gaps.

(iii) The Government may provide such results to the Contractor or Service Provider to support remediation efforts.

(iv) All benchmarks, test data, and methodologies developed or used by the Government for such assessments are considered Government Data. The government is under no obligation to disclose or provide access to the underlying data, methodologies, or systems.



GSAR Clause 552.239-7001 (pending review)

(2) Government Evaluation Rights and Remediation.

(i) The Government reserves the right to conduct automated assessments of the AI system, as deployed and configured for government users, at any time using its own benchmarks. These evaluations may assess bias, truthfulness, safety, unsolicited ideological content, and other factors determined by the Government in order to facilitate evaluations.

(ii) The Contractor must provide tools and interfaces that enable the Government to run its benchmarks in an automated fashion to test the production AI system and identify any material gaps.

(iii) The Government may provide such results to the Contractor or Service Provider to support remediation efforts.

(iv) All benchmarks, test data, and methodologies developed or used by the Government for such assessments are considered Government Data. The government is under no obligation to disclose or provide access to the underlying data, methodologies, or systems.



GSAR Clause 552.239-7001 (pending review)

(3) *Non-Compliance.*

- (i) The Government retains the right to suspend use of the AI System until performance issues are satisfactorily addressed;
- (ii) The Contractor must be liable for reasonable decommissioning costs if the agency terminates this contract for cause for failure to comply with the Unbiased AI Principles described in paragraph (i)(1).



What are legal and compliance obligations for federal contractors using AI?

Contractor Obligations (proposed GSAR):

1. Must comply with GSAR 552.239-7001 when providing AI capabilities in federal contracting
2. Must grant the government an irrevocable, royalty-free, non-exclusive license to use the AI system for the duration of the contract
3. Must not use Gov't data to fine-tune or train its AI models/machines
4. Must implement reasonable technical, administrative, organizational safeguards
5. Must report and document all AI systems used and changes
6. Must provide for human oversight
7. Must report incidents within 72 hours
8. Must establish feedback mechanisms
9. Must document its compliance for AI system decision-making, other...
10. Must advise the Government of AI model changes



What are legal and compliance obligations for federal contractors using AI?

DHS: use AI only in accordance with the Constitution and all laws

GSA: transparent governance, secure data safeguards, and tiered risk management

DOW: democratize AI experimentation, data access, competition, and responsible AI



What are the latest AI trends and developments in the federal contacting industry?

According to GAO – AI Acquisition Report

The USG doubled its use of AI between 2023-2024

AI approach in the USG is agency-specific (agency directed v. vendor-driven)

Some agencies use contracts, other agencies use other agreements

Some agencies view AI as a product, other agencies view it as a service

In the process of developing inter-agency AI information sharing (DOW, DHS, VA and GSA stated they are not required to share)



What are the latest AI trends and developments in the federal contacting industry?

Trax International Corp v. USA 1:26-cv-00796 (issue concerning technical evaluation distorted by AI hallucinations)

Venergy Group LLC v. Dept of VA, CBCA 7915, 8303 (issue concerning former employee used AI to manipulate data using CEO's information – uncovered through metadata)

Appeals of - Sayar Development Inc, ASBCA Nos. 63871, 63894, 64191, 64227 (issue concerning pro se appellant using AI to make arguments)

Ask Sage, Inc., B-423826 (issue concerning GSA improperly modified contract to make OpenAI's ChatGPT Enterprise available to agencies)



What are the most recent enforcement actions against by the U.S. Government against contractors using AI?

National Health Care Fraud Takedown Results in 455 Defendants Charged in Connection with Over \$6.5 Billion in Alleged Fraud

Regulatory Gap Between AI and Legal and Compliance Requirements

AI Driven Qui Tam Actions

DOJ's Fraud Oversight through Careful Use of Statistics (FOCUS)

"We are interested in hearing from data miners who believe they have developed particularly effective tools for detecting fraud against the government"



What are the most recent enforcement actions against by the U.S. Government against contractors using AI?

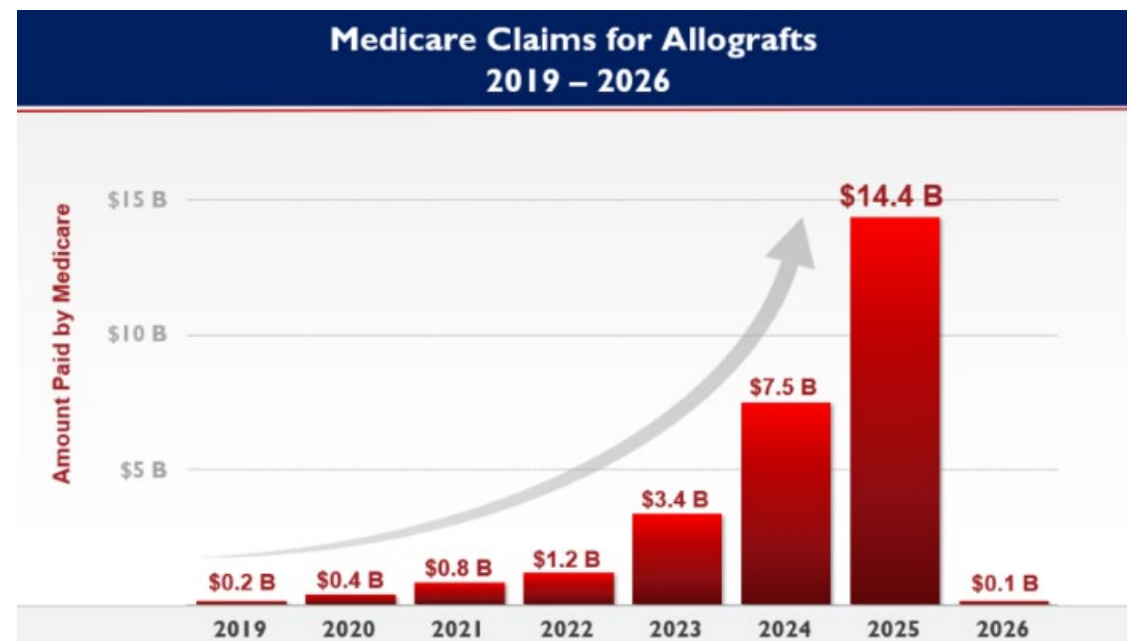
Potential AI-Enforcement Issues

Lack of AI certification / compliance

Deceptive AI claims

AI-driven billing without oversight

AI hallucinations / errors



Conclusion

The USG plans to dominate AI by dramatically increasing spending, capabilities, and competition

Promote AI while protecting the U.S. Constitution / civil rights & privacy

Lack of procurement consistency in federal contracting within the USG

Regulations and rules are behind AI developments

New and developing contractor AI-related obligations and reporting requirements

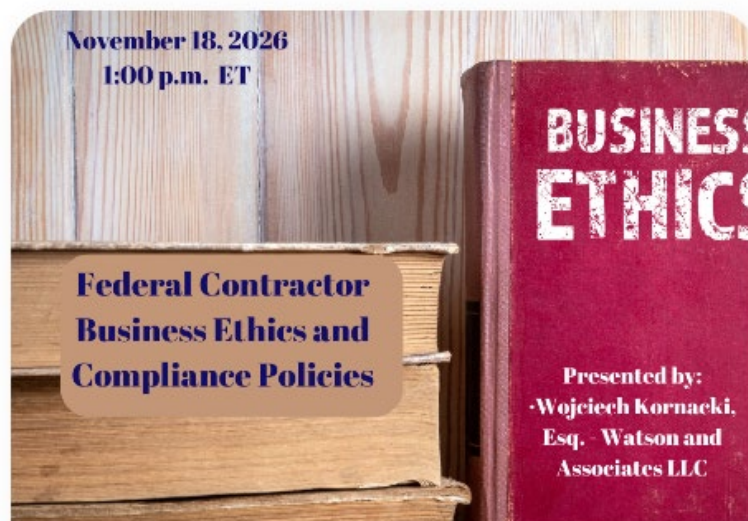
DOJ's FOCUS on Data Mining / Statistical Analysis



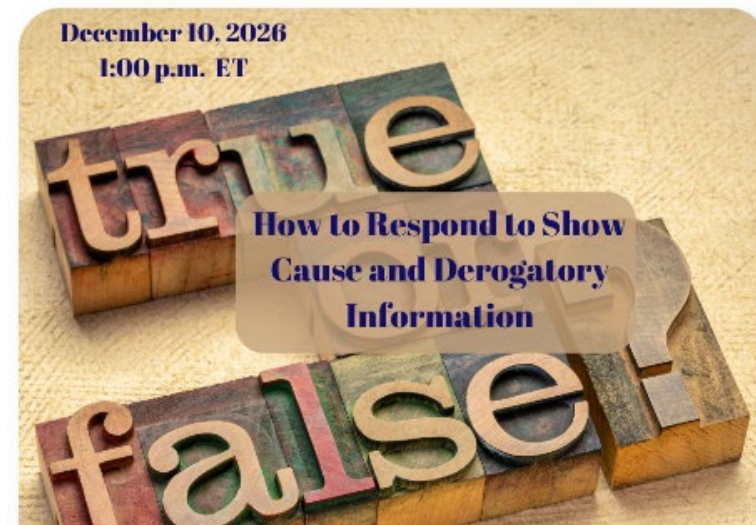
Additional Courses:



🕒 2026-10-29



🕒 2026-11-18



🕒 2026-12-10

Thank you!



Wojciech Kornacki
Government Contract and Compliance Counsel,
Of Counsel
kornackiw@theodorewatson.com | 202.640-3023





EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

April 3, 2025

M-25-22

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Russell T. Vought
Director

SUBJECT: Driving Efficient Acquisition of Artificial Intelligence in Government

1. OVERVIEW

Executive Order 13960, *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*,¹ charges Federal agencies with using safe and secure artificial intelligence (AI) in innovative ways to improve government efficiency and mission effectiveness. In carrying out this direction, agencies must procure effective and trustworthy AI capabilities in a timely and cost-effective manner. Consistent with the Advancing American AI Act,² Executive Order 14179, *Removing Barriers to American Leadership in Artificial Intelligence*,³ and Office of Management and Budget (OMB) Memorandum M-25-21, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, this memorandum provides guidance to agencies to improve their ability to acquire AI responsibly. This memorandum rescinds and replaces OMB Memorandum M-24-18, *Advancing the Responsible Acquisition of Artificial Intelligence in Government*. To that end, there are three grounding themes that drive this memorandum's requirements:

Ensuring the Government and the Public Benefit from a Competitive American AI Marketplace. Competition in the marketplace enables the government to acquire the best solutions at lower cost to the taxpayer. As agencies seek to accelerate the adoption of AI-enabled services, they must pay careful attention to vendor sourcing, data portability, and long-term interoperability⁴ to avoid significant and costly dependencies on a single vendor. The

¹ Executive Order 13960, *Promoting the Use of Trustworthy Artificial Intelligence*. December 3, 2020, <https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government>.

² Pub. L. No. 117-263, div. G, title LXXII, subtitle B, § 7224(d)(1) (codified at 40 U.S.C. 11301 note), <https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf>.

³ Executive Order 14179, *Removing Barriers to American Leadership in Artificial Intelligence*. January 31, 2025, <https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence>.

⁴ The term "interoperability" generally refers to the ability of two or more systems, products, or components to exchange information and use the information that has been exchanged, including to operate effectively together.

government must communicate clear and specific requirements that make it easy for vendors to offer state-of-the-art AI capabilities to support efficient and effective public services.

Safeguarding Taxpayer Dollars by Tracking AI Performance and Managing Risk.

AI presents a tremendous opportunity to improve government efficiency and effectiveness. To achieve this promise, agencies must ensure that the AI systems they procure are fit for purpose and deliver consistent results that preserve public trust in the manner outlined in Executive Order 13960.⁵

Promoting Effective AI Acquisition with Cross-Functional Engagement. Robust collaboration is a foundational principle of the Executive Branch’s acquisition process and remains critical for surfacing potential issues sooner rather than later to avoid obstacles and risks in procuring new technology, such as AI. The novel challenges that AI introduces require agile engagement from agency officials with varied expertise to fully address during acquisition.

2. SCOPE

The Advancing American AI Act (“the Act”) directs OMB to develop an initial means by which to ensure that contracts for the acquisition of an AI system or service align with the guidance required by the AI in Government Act of 2020, which was updated in OMB Memorandum M-25-21, and to advance the aims identified in section 7224(d)(1) of the Act. This memorandum does not supersede, and should be considered in concert with, other more general Federal policies that apply to the acquisition of AI. Agencies must comply with all applicable OMB policies and coordinate compliance across their components with all appropriate officials. Agency officials retain their existing authorities and responsibilities established in other laws and policies.

- a. **Covered Agencies.** Except as specifically noted, this memorandum applies to all agencies defined in 44 U.S.C. § 3502(1). As noted in the relevant sections, some requirements in this memorandum apply only to Chief Financial Officers Act (CFO Act) agencies, as identified in 31 U.S.C. § 901(b). The requirements in this memorandum do not apply to elements of the Intelligence Community, as defined in 50 U.S.C. § 3003.
- b. **Covered AI.** This memorandum provides requirements and recommendations that, as described in more detail below, apply to AI systems or services that are acquired by or on behalf of covered agencies.

The term *AI system*, as used in the Act and this memorandum, includes data systems, software, applications, tools, or utilities “established primarily for the purpose of researching,

This includes ensuring that open and standard data formats and application programming interfaces (APIs) are used so that foundational components can be used, including to build for new use cases, without obscure proprietary technologies or licensing.

⁵ Section 2 of Executive Order 13960 states that “[i]t is the 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.”

developing, or implementing artificial intelligence technology,”⁶ as well as data systems, software, applications, tools, or utilities where an AI capability “is integrated into another system or agency business process, operational activity, or technology system.”⁷ The term excludes, however, “any common commercial product within which artificial intelligence is embedded, such as a word processor or map navigation system.”⁸

In determining whether a product that integrates AI functionality is excepted under this provision, agencies should assess both (1) whether the product is widely available to the public for commercial use, as opposed to products that are not readily available to the general public or are specialized or customized for agency use, and (2) whether the AI is embedded in a product that has substantial non-AI purposes or functionalities, as opposed to products for which AI is a primary purpose or functionality. For example, word processing software that is primarily used for its AI functionality likely would be covered by this memorandum. On the other hand, common commercial word processing software that has substantial non-AI purposes or functionalities, but for which AI is embedded for functions like suggesting text or correcting spelling and grammar, would likely fall within the exception and thus would not be covered by the requirements of this memorandum.

This memorandum does not govern:

- i. Agencies’ regulatory actions designed to prescribe law or policy regarding non-agency uses of AI;⁹
- ii. Agencies’ assessments of particular AI applications because the AI provider is the target or potential target of a regulatory enforcement, law enforcement, or national security action; or the agency is evaluating the AI application because it was used by a criminal suspect;¹⁰
- iii. Agencies’ development of metrics, methods, and standards to test and measure AI, where such metrics, methods, and standards are for use by the general public or the government as a whole, rather than to test AI for a particular agency application;¹¹
- iv. Agencies’ acquisition of AI to carry out basic, applied, or experimental research¹² except where the purpose of such research is to develop particular AI applications within the agency; or

⁶ Pub. L. No. 117-263, div. G, title LXXII, subtitle B, § 7223(4) (codified at 40 U.S.C. 11301 note), <https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf>.

⁷ *Id.*

⁸ *Id.*

⁹ For guidance on regulatory and non-regulatory approaches to AI applications developed and deployed outside of the Federal government and best practices to reduce barriers to the development and adoption of AI technologies, agencies should consult OMB Memorandum M-21-06, Guidance for Regulation of Artificial Intelligence Applications (Nov. 17, 2020), <https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/11/M-21-06.pdf>.

¹⁰ AI is not in scope when it is the target or potential target of such an action, but it is in scope when the AI is used to carry out an enforcement action. For example, when evaluating an AI tool to determine whether it violates the law, the AI would not be in scope; if an agency was using that same AI tool to assess a different target, then the AI would be in scope.

¹¹ Examples include agency actions to develop, for general use, standards or testing methodologies for evaluating or red-teaming AI capabilities.

¹² For more information about basic, applied, or experimental research, reference the National Science

- v. AI used incidentally by a contractor during performance of a contract (e.g., AI used at the option of a contractor when not directed or required to fulfill requirements).
- c. **Future Contracts for AI.** This memorandum shall apply to any contract awarded pursuant to a solicitation issued on or after the date that is 180 days after issuance of this memorandum, as well as to any option to renew or extend the period of performance exercised on an existing contract after the date that is 180 days after the issuance of this memorandum.
- d. **Applicability to National Security Systems.** This memorandum does not apply to AI acquired for use as a component of a National Security System.¹³

3. AGENCY-LEVEL REQUIREMENTS

In addition to the actions described in Section 4 below, this memorandum directs agencies to:

- b. **Update Agency Policies.** Within 270 days of the issuance of this memorandum, agencies must revisit, and update where necessary, existing internal procedures on acquisition to comply with the requirements of this memorandum and ensure the agency's use of the acquired AI will conform to OMB Memorandum M-25-21. At a minimum, agencies must update internal procedures on acquisition to enable relevant agency officials to:
 - i. Review planned acquisitions involving an AI system or service and provide any feedback on AI performance and risk management practices as necessary, consistent with guidance in Section 4 of this memorandum;
 - ii. Convene a cross-functional team of relevant agency officials¹⁴ to include in the coordination and decision-making processes associated with the acquisition, as discussed in Section 4(a)(i) of this memorandum;
 - iii. Ensure use of appropriate contract terms for intellectual property (IP) rights, in alignment with paragraph (d) below.
- c. **Maximize the Use of American-Made AI.** Executive Order 14179 recognizes the importance of American AI development to promote human flourishing, economic competitiveness, and national security. Consistent with applicable law, it is the policy of the United States to buy American and to maximize the use of AI products and services that are developed and produced in the United States.¹⁵

Foundation's Frascati Manual. The full Frascati Manual and current and upcoming online Annexes are available at <http://oe.cd/frascati>.

¹³ The term "National Security System" has the meaning provided in 44 U.S.C. § 3552(b)(6).

¹⁴ Examples of officials with relevant equities will likely include those with expertise in acquisition (including competition advocates), IT, cybersecurity, privacy, confidentiality, civil rights, civil liberties, budgeting, data, legal, program evaluation, and other areas as necessary.

¹⁵ Executive Order 14179.

- d. **Protect Privacy.** Consistent with OMB Circular No. A-130,¹⁶ agencies shall 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). Agencies shall ensure that Senior Agency Officials for Privacy¹⁷ have early and ongoing involvement in agency acquisition or contractor use of AI involving PII, including during pre-solicitation acquisition planning and when defining requirements, to manage privacy risks and ensure compliance with law and policy related to privacy.
- e. **Protect IP Rights and Use of Government Data.** Consistent with applicable laws and government-wide policy,¹⁸ agencies must have appropriate processes for addressing use of government data and include appropriate contractual terms that clearly delineate the respective 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, fine-tune, and develop the AI system. Each agency must revisit, and update where necessary, its process for the treatment of data ownership and IP rights in procurements for AI systems or services. Agencies should prioritize standardization across contracts where possible. The Chief AI Officer Council will periodically review agency processes to encourage best practices and interagency harmonization. Agency processes should address the following:
- i. **Scope.** Scoping licensing and other IP rights appropriately, based on the intended use of AI, to avoid vendor lock-in;
 - ii. **Timeline.** Ensuring components necessary to operate and monitor the AI system or service remain available for the acquiring agency to access and use for as long as it may be necessary;
 - iii. **Data Handling.** Providing clear guidance on handling, access, and use of agency data or information to ensure, among other purposes, that such information must only be collected and retained by a vendor when reasonably necessary to serve the intended purposes of the contract;

¹⁶ See, for example, OMB Circular No. A-130, Main Body § 5(a)(1)(b)(ii) and Appendix I § 4(j)(1), https://bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf.

¹⁷ Per OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy (September 15, 2016): “At the discretion of the SAOP and consistent with applicable law, other qualified agency personnel may perform particular privacy functions that are assigned to the SAOP,” https://bidenwhitehouse.archives.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m_16_24_0.pdf.

¹⁸ See, for example: OMB Circular No. A-130 and OMB Memorandum M-25-05, *Phase 2 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Open Government Data Access and Management Guidance*, <https://www.whitehouse.gov/wp-content/uploads/2025/01/M-25-05-Phase-2-Implementation-of-the-Foundations-for-Evidence-Based-Policymaking-Act-of-2018-Open-Government-Data-Access-and-Management-Guidance.pdf>.

- iv. Use of Government Data. Ensuring contracts permanently prohibit the use of non-public inputted agency data and outputted results to further train publicly or commercially available AI algorithms, consistent with applicable law, absent explicit agency consent; and
 - v. Documentation, Transparency, and Accessibility. As noted in OMB Memorandum M-25-21, agencies, where appropriate, are encouraged, to prioritize obtaining documentation that facilitates transparency and explainability,¹⁹ and that ensures an adequate means of tracking performance and effectiveness for procured AI.
- f. Spotlight AI Acquisition Authorities, Approaches, and Vehicles.** Within 100 days of the issuance of this memorandum, GSA, in collaboration with OMB and relevant interagency councils, will develop a plan to release publicly available guide(s) to assist the acquisition workforce with the procurement of AI systems, addressing potential acquisition authorities, approaches, and vehicles as well as their potential benefits and drawbacks, and any other resources that agencies can immediately leverage for AI procurement.
- g. Contribute to a Shared Repository of Best Practices.** Within 200 days of the issuance of this memorandum, GSA, in coordination with OMB, will develop a web-based repository, available only to Executive Branch agencies, to facilitate the sharing of information, knowledge, and resources about AI acquisition. Agencies should contribute tools, resources, and data-sharing best practices developed for improved AI acquisition, which may include language for standard contract clauses and negotiated costs for common AI systems and other relevant artifacts.²⁰
- h. Determine Necessary Disclosures of AI Use in the Fulfillment of a Government Contract.** While this memorandum primarily concerns the deliberate acquisition of AI systems, vendors will likely increasingly utilize AI as part of contract performance in situations where the government may not anticipate the use of that AI. Agencies must be cognizant of the risks posed by the unsolicited use of AI systems by vendors and determine whether there are circumstances that merit including a provision in a solicitation requiring disclosure of AI use as part of any given contract's performance.

4. AI ACQUISITION LIFECYCLE GUIDANCE

The below subsections delineate requirements and recommendations for agencies as part of their AI acquisition practices. As noted above, this guidance should be considered in concert with any other relevant laws or policy that may apply to such a procurement. Throughout the AI acquisition lifecycle, agencies shall consider and mitigate, as appropriate, risks to privacy, civil liberties, and civil rights.

¹⁹ In this context, explainability refers to an agency's ability to provide evidence or reasons for system output. A significant enabler of explainability is clear documentation that is meaningful or understandable to individual users and reflects the process for model-driven development.

²⁰ Examples of other relevant artifacts might include negotiated costs for common AI systems, best practices for performance-based acquisition, and approaches for structuring and including provisions related to data and model documentation, availability, and transparency to support ongoing performance monitoring, testing and evaluation, and program evaluation to ensure effective and efficient deployment and service delivery.

a. Identification of Requirements.

- i. Convening a Cross-Functional Team. Based on the nature of the requirements involved in the procurement, agencies should follow their designated process for convening an internal cross-functional team, as required by Section 3(a).²¹ This team should then work to inform the procurement of AI systems or services in a streamlined manner that apportions time and resources according to the requirements of the procurement, including associated complexity and risk, to support effective, efficient, and responsible development and execution of ongoing performance monitoring. The team should assist in creating an initial list of potential risks that should be evaluated based on the type of AI system or service under consideration. In particular, the team must identify potential risks to the agency's implementation of the nine principles for use of AI in government articulated in Executive Order 13960.²²
- ii. Determining the Use of High-Impact AI. During this phase, agencies must identify reasonably foreseeable use cases arising from the use of an AI system or service, and to the greatest extent practicable, make an initial determination of whether a system is likely to host high-impact AI use cases, as defined by OMB Memorandum M-25-21.²³ This initial determination will assist in developing key questions to investigate as part of market research.

b. Market Research & Planning.

- i. Broad Market Research. Agencies should take advantage of the dynamic evolution of the AI market to seek state-of-the-art AI capabilities by conducting thorough market research. As part of this work, agencies should seek to leverage existing interagency knowledge sharing and acquisition platforms across the Executive Branch. They should also, when appropriate, seek out novel AI capabilities from new entrants that have not previously considered working with the Executive Branch. To support market research, OMB will develop additional "playbooks" specific to various types of AI (e.g., AI-based biometrics, specialized computing infrastructure, and generative AI), designed to highlight the particular considerations and nuances inherent in these specialized areas.

²¹ Refer to the list identified in Footnote 13 regarding the potential makeup of such teams.

²² Executive Order 13960, *Promoting the Use of Trustworthy Artificial Intelligence*. December 3, 2020, <https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government>.

²³ The term "high-impact AI" has the meaning provided in OMB Memorandum M-25-21, as AI with an output that serves as the primary basis for decisions or actions with legal, material, binding, or significant effect on: an individual or entity's civil rights, civil liberties, or privacy; or an individual or entity's access to education, housing, insurance, credit, employment, and other programs; or an individual or entity's access to critical government resources or services; or human life, well-being; or critical infrastructure or public safety; or strategic assets or resources, including high-value property and information marked as sensitive or classified by the Federal Government.

- ii. Product Demonstration. Where practicable, agencies should seek detailed demonstrations and tests of potentially useful AI systems or services in scenarios that closely reflect the intended real-world operating environment, including the specific characteristics of agency networks. These demonstrations should be used to help interrogate capabilities and limitations of a given provider. This phase should also serve as an opportunity to identify any obstacles to long-term cost-effectiveness with regard to vendor lock-in.²⁴
- iii. Performance-Based Acquisition Techniques. Agencies are strongly encouraged to use performance-based techniques, as outlined below, to identify requirements and contract terms. Resulting performance-based requirements allow agencies to understand and assess vendor claims about their proposed use of AI systems or services prior to contract award, acquire AI capabilities that address their needs, and perform post-award monitoring. Focusing acquisition on achieving desired performance outcomes directly facilitates an agency's ability to ensure its needs are met by defining metrics to maintain and improve performance of the AI system or service. Performance-based techniques include:
 - A. *Statements of Objectives (SOO) and Performance Work Statements (PWS)*. SOO and PWS provide agencies with more flexibility to acquire AI systems or services that meet agencies' outcome-based needs, but may not meet unnecessary or overly-limiting requirements in Statements of Work (SOW).
 - B. *Quality Assurance Surveillance Plans (QASP)*. QASPs can help agencies overcome challenges in defining relevant performance metrics pre-solicitation and can enable a more collaborative process for negotiating a QASP that meets agency needs and objects. Government personnel should be prepared to assume a more active role in performance monitoring.
 - C. *Contract incentives*. Contract incentives can be used to improve the performance and interoperability of AI systems and services. Incentives can be based on metrics and provisions in QASPs. When determining whether to include performance-based incentives, agencies must carefully consider whether the established metrics are correctly tied to desired business and mission outcomes, and whether they can adequately measure baseline performance of the AI systems or services.

c. Solicitation Development.

- i. AI Use Transparency Requirements. When practicable, agencies must disclose in solicitations whether a planned use of an AI system meets the threshold of a high-impact use case or if there is a reasonable likelihood for such a high-impact use case to

²⁴ This recommendation generally refers to approaches to storing and representing data and models in a manner that allows for them 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.

occur during the life of the contract. Additionally, for AI systems with potential or expected high-impact use cases, agencies must inform vendors of reasonable transparency and documentation requirements that will be placed on the vendor to enable agency compliance with the requirements in OMB Memorandum M-25-21. For example, agencies should require sufficient descriptive information from vendors to complete the required AI Impact Assessment for high-impact use cases.

- ii. Protections Against Vendor Lock-In. In general, agencies should include provisions in the solicitation reflecting the agency's interest in AI proposals that reduce the risk of vendor lock-in, such as requirements regarding knowledge transfer, clear data and model portability practices, clear licensing terms, and pricing transparency.²⁵
- iii. IP Rights and Use of Government Data. Consistent with the processes developed pursuant to section 3(d) above, agencies must include appropriate terms related to IP rights and lawful use of government data.

d. Selection and Award

- i. Testing and Evaluation. When evaluating proposals agencies must, to the greatest extent practicable, test proposed solutions to understand the capabilities and limitations of any offered AI system or service. As part of this work, agencies should consider whether it is appropriate to create a testing environment in agency networks specifically to enable testing of proposed solutions on government-owned systems.
- ii. Opportunity and Risk Re-Evaluation. Prior to selection, agencies should assess proposals for potential new AI-related risks that were not previously identified and should review proposals for any challenges that might arise with compliance requirements identified in OMB Memorandum M-25-21.
- iii. Contract Terms. Consistent with law and government-wide policy, where applicable, agencies must include terms that address the following in contracts for AI systems and services:

²⁵ To promote cost-effectiveness and foster competition, there are several vendor practices agencies can seek to leverage as evaluation criteria. Some examples include the use of well-defined application programming interfaces (APIs), particularly within acquired architectures, that promote interoperability with other elements of the technical stack; robust documentation regarding decisions related to foundational model development, coding languages used, testing scripts and protocols, and other decisions related to the development of AI tools in a developer experience framework that facilitates the transition of AI tools from one vendor to the next; open-source licenses to vendor's products, including AI models, AI systems, AI services, and datasets; and transparent and non-discriminatory pricing practices. Examples of the latter practices include offering products without bulk pricing arrangements, tying arrangements, steering arrangements, minimum spend requirements, or other agreements that encourage consolidation of spending with one vendor or one group of vendors through fixed contract lengths, exclusive discounts, or other incentives; offering systems or services at uniform and publicly available prices and not engaging in self-preferencing; providing equal access on comparable terms to downstream businesses, such as by refraining from self-preferencing vertically integrated systems or services; and providing information about which subcontractors, including system integrators, were engaged, how they were selected, and how their involvement impacts price.

- A. *IP Rights and Use of Government Data.* Terms on this subject must be consistent with the processes adopted by the agency per Section 3(d) above.
- B. *Privacy.* Privacy considerations are described in Section 3(c) of this memorandum.
- C. *Vendor Lock-In Protections.* As described identified during solicitation development, terms on this subject are necessary to reduce the risk that switching vendors could become cost-prohibitive. Protections against vendor lock-in can vary, but include requirements for vendor knowledge transfers, data and model portability, providing agencies with rights to code and models produced in performance of a contract, and transparency in licensing and pricing.
- D. *OMB Memorandum M-25-21 Compliance Requirements.* Contracts must ensure compliance with minimum risk management practices for high-impact use cases as required under M-25-21.
- E. *Ongoing Testing and Monitoring.* Contractual terms must provide the contracting agency the ability to regularly monitor and evaluate (e.g., on a quarterly or biannual basis, based on the needs of the program) performance, risks, and effectiveness of an AI system or service. To achieve that outcome:
 - I. Agencies must use data they have defined (e.g., agency validation and testing datasets) when conducting any independent evaluations to ensure the AI system or service is fit for purpose. The data used when conducting independent evaluations should not be accessible to the vendor, and should be as similar as possible to the data used when the system is deployed;
 - II. Vendors must provide the access and time necessary for agencies to complete independent evaluation. Alternatively, agencies may allow vendors to complete that testing when most appropriate, but must closely monitor such instances and require testing results detailed enough for the testing to be independently verified or reproduced, if practicable; and
 - III. Contracts must detail the examination, testing, and validation procedures of the vendor and must not prohibit agencies from internally disclosing how the vendor conducts testing or the results of testing.
- F. *Vendor Performance Requirements.* Federal agencies are encouraged to require vendors to regularly monitor an AI system's performance and rectify behavior defined as unacceptable, require vendors to meet performance standards before deploying a new version of an AI system or service or to roll-back to a previous version if a new version fails to meet performance standards, and incentivize model satisfactory performance through performance-based contracting.
- G. *New Feature Notification.* As required by Section 3(g), agencies should consider, where relevant, requiring vendors to provide a notification to relevant agency stakeholders prior to the integration of new AI enhancements, features, or

components into systems and services being delivered under contract. Vendor notification to agencies should follow existing processes, where practicable, and should be determined by the relevant agency stakeholders. Agencies should also ensure, prior to release, that compliance requirements will be followed, consistent with OMB Memorandum M-25-21.

e. Contract Administration

- i. Authorization To Operate Compliance. Consistent with the requirements of OMB Circular No. A-130 and other policies established pursuant to the Federal Information Security Modernization Act, any AI systems and services operated as an information system by or on behalf of an agency must receive an authorization to operate from an appropriate agency official prior to deployment.²⁶
- ii. Contractual Oversight. Agencies must perform effective system oversight consistent with the terms of the contract. This includes monitoring system performance to ensure that any emerging risks to privacy, civil rights, and civil liberties are identified and mitigated as appropriate.
- iii. Performance and Cost Justification. As part of contract administration, agencies should, to the extent practicable, arrange for periodic evaluation of the AI system or service's value to the government. Such an evaluation should take into account comparative system effectiveness and efficiency for purpose, the risk associated with use, and any ongoing operation and maintenance costs. Where practicable, agencies should consider terms to solicit and incorporate feedback from end users, program managers, and other relevant stakeholders to inform modifications that continuously improve performance of the AI system or service in the context of the agency's mission.
- iv. Sunset Criteria. Where practicable, agencies should determine criteria for sunsetting the use of an AI system. Changes in costs, agency needs, vendor-proposed requirements, or model performance may signal that an agency should reconsider continued use.

f. Contract Closeout

- i. Vendor Lock-In Protection. As soon as a decision is made not to extend a contract for an AI system or service, agencies should work with the vendor to implement any contractual terms related to ongoing rights and access to any data or derived products resulting from the services provided under the contract. This includes ensuring a mutual understanding of format and usability of any data, and any circumstances that

²⁶ See 44 U.S.C. § 3554 (making agency heads responsible for providing appropriate information security protections for Federal information and information systems); *see also* OMB Circular No. A-130, Appendix I § (4)(d) (requiring senior Federal officials at agencies to complete authorizations to operate for each information system).

could result in expiration of access, as well as a plan for conducting any transfers of data or other derived assets necessary per the terms of the contract.

Appendix I: Consolidated Table of Required Actions

Responsible Entity	Action	Section	Deadline
GSA, in coordination with OMB	Develop a plan to release a publicly available guide on their website to assist agencies with AI procurement.	3(e)	100 days
Each agency	Achieve full compliance with the guidance of this memorandum.	2(c)	180 days
Each agency	Include the process by which the agency will standardize the treatment of data ownership and IP rights in procurements for AI systems or services as part of policy and process updates.	3(d)	200 days
GSA, in coordination with OMB	Develop a web-based repository of tools and resources to enable AI procurement.	3(f)	200 days



SECRETARY OF WAR
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

JAN - 9 2026

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOW FIELD ACTIVITY DIRECTORS

SUBJECT: Artificial Intelligence Strategy for the Department of War

Accelerating America's Military AI Dominance

President Trump makes clear in Executive Order 14179, "It is the policy of the United States to sustain and enhance America's global Artificial Intelligence (AI) dominance in order to promote human flourishing, economic competitiveness, and national security." In the national security domain, AI-enabled warfare and AI-enabled capability development will re-define the character of military affairs over the next decade. This transformation is a race — fueled by the accelerating pace of commercial AI innovation coming out of America's private sector. The United States Military must build on its lead over our adversaries in integrating this technology, established during President Trump's first term, to make our Warfighters more lethal and efficient. To this end, aligned with America's AI Action Plan, I direct the Department of War to accelerate America's Military AI Dominance by becoming an "AI-first" warfighting force across all components, from front to back.

The Department will achieve this objective by:

- Unleashing experimentation with America's leading AI models Department-wide, and rewarding AI-first re-conceptions of legacy approaches;
- Aggressively identifying and eliminating bureaucratic barriers to deeper integration, which are vestiges of legacy information technology and modes of warfare;
- Focusing our investment to leverage America's core asymmetric advantages in AI computing, model innovation, entrepreneurial dynamism, capital markets, and combat-proven operational data from two decades of military and intelligence operations that no other military can replicate; and
- Executing a set of "Pace-Setting Projects" (PSPs) that will demonstrate the accelerated pace of execution, focus, and ethos we need to stay ahead. The PSPs will also serve as tangible, outcome-oriented vehicles for rapidly completing our buildout of the foundational AI enablers (infrastructure, data, models, policies, and talent) needed to accelerate AI integration across the entire Department.



The seven initial PSPs outlined below establish the new execution standard: single accountable leaders, aggressive timelines, measurable outcomes, and rapid iteration where failure accelerates learning and improvement.

Acceleration Approach

The means we will employ to pursue this strategy will continue to encompass our substantial program funding and workforce focused on AI across the Services and Components. We will also use the timely financial resources provided by Congress in the form of One Big Beautiful Bill, along with expanded budget withhold (Joint Acceleration Reserve) flexibility, to catalyze our accelerated pace of Military AI integration in the immediate term. And we will leverage the access, capabilities, investments, and insights of America's allies and partners to support our shared objectives, consistent with the President Trump's AI Action Plan to "Lead in International AI Diplomacy and Security".

We will re-focus the Chief Digital and AI Office (CDAO) and these enhanced resources to unlock critical foundational enablers needed to accelerate war-winning efforts across the Department, starting with enabling the set of seven PSPs listed below in fiscal year 2026. These PSPs will address key opportunities for enhanced military AI advantage across Warfighting, Intelligence, and Enterprise mission areas:

- **Warfighting:**

1. Swarm Forge: Competitive mechanism to iteratively discover, test, and scale novel ways of fighting with and against AI-enabled capabilities — combining America's elite Warfighting units with elite technology innovators.
2. Agent Network: Unleashing AI agent development and experimentation for AI-enabled battle management and decision support, from campaign planning to kill chain execution.
3. Ender's Foundry: Accelerating AI-enabled simulation capabilities — and sim-dev and sim-ops feedback loops — to ensure we stay ahead of AI-enabled adversaries.

- **Intelligence:**

4. Open Arsenal: Accelerating the TechINT-to-capability development pipeline, turning intel into weapons in hours not years.
5. Project Grant: Enabling transformation of deterrence from static postures and speculation to dynamic pressure with interpretable results.

- **Enterprise:**

6. GenAI.mil: Democratizing AI experimentation and transformation across the

Department by putting America's world-leading AI models directly in the hands of our three million civilian and military personnel, at all classification levels.

7. Enterprise Agents: Building the playbook for rapid and secure AI agent development and deployment to transform enterprise workflows.

The PSPs will each be led by an exemplary program leader in partnership with a sponsoring organization. Progress will be demonstrated monthly to the Deputy Secretary of War (Deputy Secretary) and Under Secretary of War for Research and Engineering (USW(R&E)), with initial demonstration by transition-partner user(s) to occur within six months from the date of this memorandum.

The CDAO will also ensure all foundational enablers unlocked by these projects are made available to programs Department-wide in real-time, so accelerated execution by PSPs will enable projects across the Department to accelerate their pace along with them. Therefore, I direct each Military Department, combatant command, and defense agency and field activity to identify within 30 days at least three projects they will prioritize to fast-follow these PSPs. Efforts under the Department's six Critical Technology Areas — including autonomy, C-C5ISR, and advanced manufacturing — must continue to push the pace for the Department of War (DoW). And the special initiatives outlined in classified annexes, including those in the Classified Annex provided by separate cover to this memorandum, will also be accelerated. CDAO will track and rank this extended pack of AI efforts by speed and impact, and progress will be reported monthly to the Deputy Secretary and USW(R&E).

AI Compute. As part of our AI and Autonomy acceleration investments, the Department will invest substantial resources in the expansion of our access to AI compute infrastructure, from datacenters to the edge. We will leverage the hundreds of billions in private sector capital investment being made in America's AI sector through our growing array of creative partnerships with America's world-leading companies. We will work with interagency partners to establish technical standards for new secure datacenters. And we will support and leverage the American Science and Security Platform being developed by President Trump's Genesis Mission for science and technology innovation, so our warfighters and capability developers have the full benefit of America's AI compute resources and latest innovations.

Data Access. I direct the CDAO to enforce, and all DoW Components to comply with, the 'DoD Data Decrees' to further unlock our data for AI exploitation and mission advantage. Military Departments and Components will establish, maintain, and update federated data catalogs exposing their system interfaces, data assets, and access mechanisms across all classification levels, as mandated by the Department's May 2021 memorandum, "Creating Data Advantage." They will deliver their current catalogs — with all available updates — to the CDAO within 30 days of the date of this memorandum. The Under Secretary of War for Intelligence and Security will ensure intelligence data receives parallel treatment, with exploitation pathways established within the same timeframe. The CDAO is authorized to direct release of any DoW data to cleared users with valid purpose, consistent

with security guidelines. Effective immediately, denials of CDAO data requests must be justified to the USW(R&E) within seven (7) days, who will remediate or escalate to the Deputy Secretary. Our data advantage is meaningless if our developers and operators cannot exploit it.

Talent. Finally, I believe the best American talent will see this accelerated posture of AI capability development and adoption at the DoW, and I expect each Service and Component to attract and retain this talent. To that end, I direct use of special hiring and pay authorities Department-wide, as well as novel talent programs from the Office of Personnel and Management and other partners, to accelerate our pace of technical talent hiring into AI roles. And I direct each Component to provide AI hiring and talent development plans to the Under Secretary of War for Personnel and Readiness within 60 days of this memo for approval, denial or modification within 30 days thereafter.

Acceleration Expectations

This strategy will accelerate our advantage, and we must implement it with the Warrior Ethos. Consistent with the refocusing of the Department onto a wartime footing, I expect the following approaches to become internalized as essential elements of our execution in this race to maintain Military AI Dominance:

Speed Wins. We must internalize that Military AI is going to be a race for the foreseeable future, and therefore speed wins. We must weaponize learning speed, and measure and manage cycle time and adoption rates as decisive variables in the AI era. We must accept that the risks of not moving fast enough outweigh the risks of imperfect alignment. I direct CDAO to establish deployment velocity and operational cycle-time metrics for all PSPs, to be a focus of their monthly reporting to the Deputy Secretary and USW(R&E).

AI Model Parity. We are seeing unprecedented velocity in the evolution of the frontier AI models. These models are becoming smarter and more robust every day. The Department cannot be working off models that are months or years old. We must have the latest and greatest AI models deployed for our warfighters. Deploying these capabilities across all echelons is simply not enough, we must be able to support and sustain rapid model updates across all echelons. I direct CDAO to establish a delivery and integration cadence with AI vendors that enables the latest models to be deployed within 30 days of public release. This shall be a primary procurement criterion for future model acquisition.

Wartime Approach to Blockers. We must eliminate blockers to data sharing, Authorizations to Operate (ATOs), test and evaluation and certification, contracting, hiring and talent management, and other policies that inhibit rapid experimentation and fielding. We must approach risk tradeoffs, “equities”, and other subjective questions as if we were at war. To this end, I expect our CDAO to act as a Wartime CDAO and work with the Chief Information Officer to fully leverage statutory and delegated authorities to accelerate AI capability delivery, including cross-domain data access and rapid ATO reciprocity on behalf of pace-pushing leaders across the Department. The USW(R&E) will establish a monthly "Barrier Removal Board" with authority to waive non-statutory requirements and escalate

blockers for immediate resolution.

Competition > Centralized Planning. As America's AI ecosystem demonstrates, robust competition by small teams, with transparent metrics for results, is the engine of commercial AI leadership. We must bring this model into the Department and encourage robust competition to spur faster military AI integration. Small, accountable teams will win over process in a race characterized by dynamic and unpredictable innovation. We will measure success through continuous field experimentation: putting AI capabilities in operators' hands, gathering feedback within days not years, and pushing updates faster than the enemy can adapt. I direct CDAO to establish AI system usage and mission impact metrics for evaluating the success of these AI acceleration efforts. To enable market dynamics to drive resourcing, decisions about future resourcing and deprecation of associated capabilities will principally be made on the basis of these metrics.

AI-Native Warfighting. Together with capability innovation, we must more fully incorporate AI and Autonomy into military planning; tactics, techniques and procedures (TTP) development; and experimentation processes. I direct each Service Chief and Combatant Commander to designate an AI Integration Lead within 30 days, who will work with the CDAO and be responsible for the co-evolution of AI-enabled capabilities with warfighting concepts and experimentation. I direct CDAO to establish criteria for robust experimentation with AI capabilities. And I direct the Joint Staff to designate a senior official to monitor Service AI warfighting concept development and workflow optimization, and provide me with progress reports on a quarterly basis. We must put aside legacy approaches to combat and ensure we use this disruptive technology to compound the lethality of our military. Exercises and experiments that do not meaningfully incorporate AI and autonomous capabilities will be reviewed by the Director of Cost Assessment and Program Evaluation for resourcing adjustment.

Modular Open Architectures. In the AI arms race, system architectures must enable component replacement at commercial velocity to maintain overmatch. I direct Military Department and Component Program Managers acquiring AI capabilities to enforce Modular Open System Architectures (MOSA) along with the "DoD Data Decrees," exposing modular interfaces and associated documentation sufficient for third-party integration without prime contractor support.

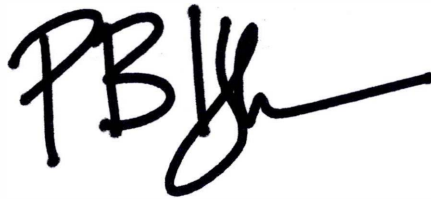
Clarifying "Responsible AI" at the DoW — Out with Utopian Idealism, In with Hard-Nosed Realism. Diversity, Equity, and Inclusion and social ideology have no place in the DoW, so we must not employ AI models which incorporate ideological "tuning" that interferes with their ability to provide objectively truthful responses to user prompts. The Department must also utilize models free from usage policy constraints that may limit lawful military applications. Therefore, I direct the CDAO to establish benchmarks for model objectivity as a primary procurement criterion within 90 days, and I direct 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. I also direct the CDAO to ensure all existing AI policy guidance at the Department aligns with the directives laid out in this memorandum.

Becoming An AI-First Department

The time is now to accelerate AI integration, and we will put the full weight of the Department's leadership, resources, and expanding corps of private sector partners into accelerating America's Military AI Dominance.

Becoming an "AI-First" warfighting force requires more than integrating AI into existing workflows. It requires re-imagining how existing workflows, processes, TTPs, and operational concepts would be designed if current AI technology existed when they were created — and then re-inventing them accordingly.

We must drive this transformation across every aspect of the Department. The expectations outlined above must become technological "AI fitness standards" for our Joint Force. 2026 will be the year we emphatically raise the bar for Military AI Dominance.

A handwritten signature in black ink, consisting of the letters 'PBJh' followed by a long horizontal stroke.

RELEASE
IMMEDIATE RELEASE

Department of War Launches OpenAI's ChatGPT Mil on GenAI.mil

Aug. 31, 2026

The Department of War today launched OpenAI's ChatGPT Mil, marking it as the next frontier AI capability housed on GenAI.mil, the Department's premier generative AI platform. This milestone represents the adoption phase of an enterprise partnership established between the Department and OpenAI in 2025. Accredited for Controlled Unclassified Information (CUI) at Impact Level 5 (IL5), ChatGPT Mil is engineered for secure, consistent enterprise use.

ChatGPT Mil brings a familiar commercial experience into the Department's secure environment, tailored to warfighter needs. The core experience centers on chat, files, projects, and custom GPTs, with additional features sequenced over time. ChatGPT Mil supports document-heavy unclassified work across the Department, including planning, policy, logistics, and administration, and is built for scale to support more than 3 million Department personnel. This deployment accelerates routine tasks and frees up time for more critical projects across the Joint Force. Integrating ChatGPT Mil into GenAI.mil alongside existing frontier AI capabilities establishes a robust, multi-model ecosystem for the warfighter.

Through the Chief Digital and AI Office (CDAO) and the Office of the Under Secretary of War for Research and Engineering, the Department will continue scaling frontier AI as a

force multiplier across the Joint Force. This launch supports the White House's AI Action Plan and reinforces the Department of War's commitment to leading the adoption of AI for warfighter mission sets and decision superiority.

Hosted by WEB.mil

compliance obligations. In assessing the cost of compliance for small entities and for IPCS providers of all sizes, WCB/OEA are not in a position at this time to determine whether the proposed 2026 Mandatory Data Collection will impose any significant costs for compliance in general, or to quantify those costs. We anticipate that the information we receive in comments will help the Commission identify and evaluate relevant compliance matters for small entities, including compliance costs and other burdens that may result from the proposals and inquiries we make in the Public Notice.

E. Discussion of Significant Alternatives Considered That Minimize the Significant Economic Impact on Small Entities

The RFA directs agencies to provide a description of any significant alternatives to the proposed rules that would accomplish the stated objectives of applicable statutes, and minimize any significant economic impact on small entities. The discussion is required to include alternatives such as: “(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities.”

The proposed 2026 Mandatory Data Collection is a one-time request and does not impose a recurring obligation on providers. Because the Commission’s 2025 *IPCS Order* requires all IPCS providers to comply with the 2026 Mandatory Data Collection, the collection will affect smaller as well as larger IPCS providers. WCB/OEA have taken steps to ensure that the data collection template is competitively neutral and not unduly burdensome for any set of providers. For example, in the Public Notice, WCB/OEA propose to collect data for a single calendar year instead of multiple years. WCB/OEA also propose to eliminate or streamline various reporting requirements that had been required in previous data collections. Additionally, WCB/OEA seek comment on whether there are additional ways to minimize the burdens of the data collection on providers while ensuring that the Commission obtains the data needed to meet its goals.

WCB/OEA will consider the economic impact on small entities, as identified in

comments filed in response to the Public Notice and this Supplemental IRFA, in reaching final conclusions and finalizing the instructions, templates, and certification form for the proposed 2026 Mandatory Data Collection.

F. Federal Rules That May Duplicate, Overlap, or Conflict With the Proposed Rules

None.

V. Proposed 2026 Mandatory Data Collection Instructions, Templates, and Certification Form

The instructions, template, and certification form for the proposed 2026 Mandatory Data Collection are available through this link: <https://www.fcc.gov/sites/default/files/2026IPCS%20MDC%20proposedInstructions.docx>.

Federal Communications Commission.

Lynne Engledow,

Chief, Pricing Policy Division, Wireline Competition Bureau.

[FR Doc. 2026–12234 Filed 6–16–26; 8:45 am]

BILLING CODE 6712–01–P

GENERAL SERVICES ADMINISTRATION

48 CFR Parts 539 and 552

[Notice–MVAC–2026–01; Docket No. 2026–0331; Sequence No. 1]

General Services Acquisition Regulation; Acquisition of Information and Communication Technology; Notice of Listening Sessions and Request for Comments

AGENCY: Office of Acquisition Policy, General Services Administration (GSA).

ACTION: Proposal; request for comments.

SUMMARY: The General Services Administration (GSA) is seeking public comment on the draft of a new General Services Administration Acquisition Regulation (GSAR) clause regarding basic safeguarding of data within Large Language Model Artificial Intelligence Systems (LLMs). Due to the complexity of the issue, GSA is publishing this notification and draft clause to gather feedback from stakeholders before taking future action (e.g., deviation and/or formal rulemaking).

DATES:

Comment due date: Interested parties should submit written comments as noted below on or before August 3, 2026, to be considered in the formation of the final GSAR clause.

Public listening session date: GSA plans to hold a public listening session on Tuesday, July 14, 2026. For

additional information see section D of the **SUPPLEMENTARY INFORMATION**.

ADDRESSES: GSA invites interested persons to submit comments on this notification via the Federal eRulemaking portal at <https://www.regulations.gov>. This website provides the ability to type short comments directly into the comment field or attach a file for lengthier comments. Submit comments by searching for “Notice–MVAC–2026–01” and follow the instructions on the site. Please include your name, company name (if any), and “Notice–MVAC–2026–01” on your attached document. To confirm receipt of your comment(s), please check www.regulations.gov, approximately two-to-three days after submission to verify posting.

If your comment cannot be submitted using <https://www.regulations.gov>, call or email the points of contact in the **FOR FURTHER INFORMATION CONTACT** section of this document for alternate instructions.

Please note that all public comments received are subject to the Freedom of Information Act and will be posted in their entirety, including any personal and/or business confidential information provided. Do not include any information you would not like to be made publicly available. All statements received, including attachments and other supporting materials, are part of the public record and subject to public disclosure. You should submit only information that you wish to make available publicly.

Public Listening Session

The Listening Session will be held from 11 a.m. to 2 p.m. ET, at The George Washington Law School, Room Lerner 201, 2000 H Street NW, 20052. For additional information see section D of the **SUPPLEMENTARY INFORMATION**.

FOR FURTHER INFORMATION CONTACT: For questions about this request for comments, please contact Ms. Johnnie McDowell at 202–718–6112 or via email at gsarpolicy@gsa.gov. For questions about the listening session, please email frederick.landry@gsa.gov.

SUPPLEMENTARY INFORMATION:

A. Background

The rapid advancement and adoption of Large Language Model Artificial Intelligence (LLM) systems present both unprecedented opportunities and significant challenges for Federal agencies. As GSA establishes contracts for these technologies, ensuring the integrity, security, and appropriate handling of Government Data is paramount. This notification introduces a new GSAR clause, 552.239–7001,

“Basic Safeguarding of Data within Large Language Model Artificial Intelligence Systems (LLMs),” to address these critical concerns. This clause may be used in GSA’s Government-wide contracts (e.g., Federal Supply Schedule, GWACs, and OASIS+).

This clause is developed in response to the growing use of LLMs across Government and the need for a standardized approach to data protection, intellectual property, and ethical AI development when LLM’s are used to process Government data. It is informed by principles outlined in Executive Orders (e.g., Executive Order 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* and OMB Memorandums (e.g., OMB memorandum M–25–22, *Driving Efficient Acquisition of Artificial Intelligence in Government*, and comments received on the first draft of this clause. The first draft was issued through GSA Interact on January 12, 2026 (https://buy.gsa.gov/interact/community/6/activity-feed/post/4d70761f-60f8-4eb0-8119-052ec4c7c9b3/Advanced_Note_for_MAS_Refresh_31_and_Upcoming_Mass_Modification).

The updated draft of the clause can be found below.

B. Discussion of Proposed Changes

GSA proposes to add GSAR clause 552.239–7001 to establish comprehensive requirements for the basic safeguarding of Government Data within LLM systems when they process Government data. The clause reflects substantial revisions from the January 12, 2026, version and reflects GSA’s understanding of comments and concerns on that version.

Key Changes

In addition to other updates, GSA implemented the following changes as a response to industry comments:

Scope

- Clarified the scope of the clause by:
 - Changing the name of the clause to “Basic Safeguarding of Data within Large Language Model Artificial Intelligence Systems (LLMs)”.
 - Clarifying that the clause only applies when LLMs process Government data.
 - Adding exceptions.
 - Establishing a new section entitled “Applicability and Flowdown” (paragraph (a)). This section clarifies when the clause applies (when Government Data is processed by an LLM) and when it does not (LLMs embedded in common commercial

products or when LLM functionality is incidental).

- The clause is updated to establish common roles involved with various functions within the LLM supply chain (i.e., LLM Developers, LLM System Operators, LLM System Integrators, and LLM Service Providers) and mandates the flowdown of specific paragraphs/requirements within the basic clause to any subcontractor or service provider functioning within common applicable roles. The goal is to ensure data safeguarding responsibilities are extended appropriately throughout the complex ecosystem of LLM development and deployment.

Definitions

Expanded and clarified definitions as follows:

- *Contractor*: Clarified the term for both prime contractors and subcontractors in the context of required flowdown requirements.
- *Data, Data Inputs, Data Outputs, Government Data*: Clarified the scope for what constitutes Government information within the LLM context, including user prompts, queries, generated responses, and derived data.
- Established definitions for LLM System Integrator, LLM System Operator, LLM Developer, LLM Service Provider, Background Data, and Material Change.

Contractor Responsibilities

- Clarified requirements for contractor responsibilities, government data use and handling, licensing requirements, and compliance requirements.

Compliance, Reporting, and Documentation

- Identified the contractor and flowdown roles regarding compliance, reporting and documentation including timeframes.

Change Notification

- The term “change management” was changed to “Change Notification” (paragraph “i” of the clause) to better describe the requirement. Clarifying language was added to ensure that contractors know what, when, and how to notify GSA of changes to the LLM.

Unbiased AI Principles

- The draft provides more context to the application of “unbiased AI principles” (paragraph “j” of the clause).

C. Specific Questions for Comment

To understand the scope of the impact of this clause and how this impact could

be affected in subsequent actions (e.g., deviation and/or rulemaking), GSA welcomes input on the following questions in addition to all other comments you want GSA to consider:

1. Does the change in clause prescription adequately address previous concerns about the broadness of the scope of the clause?
2. Are the requirements such as Government data ownership and protection and contractor accountability clearly defined?
3. Are the roles and responsibilities of the contractor, LLM Developer, LLM System Operator, LLM System Integrator, and LLM Service Provider clearly defined and flowdown paragraphs accurately presented?
4. Do you understand how to implement the flowdown clauses?
5. Does the clause adequately address risks related to foreign ownership or control of LLMs, where changes to the LLM could covertly affect Government Data, outputs, or decisions without changing the contracting entity?

Format of Responses

When submitting comments, please identify the specific page number, section, and paragraph (e.g., page 5, (c)(1)(i), flowdown clause number, etc). For each entry, include any administrative burdens, reasons for disagreement or support, and suggested language. Additionally, where applicable, please provide citations and sources that support your recommendations.

For ease of reading and standardization, the use of a spreadsheet to format (e.g., company name, identify specific paragraph, copy of exact language in dispute, suggested language, comment, citation, if any) is encouraged. If commenters identify benefits, costs, burdens, loopholes, or shortcomings of particular options for implementing the clause, GSA requests that commenters provide data and evidence to support the comments.

D. Listening Session Registration

Industry partners wishing to attend in-person or virtually must register. Registration will close on Friday, July 3, 2026. In-person attendance space is limited and will be on a first-come, first-served basis. Once the maximum in-person attendance registration has been reached, all other registrants will be registered for virtual attendance. Registrants who would like to present information on topics must register in advance and registration will close on Friday, July 3, 2026.

GSA invites a wide range of perspectives to discuss how we can

improve the draft clause. We want to hear about its strengths, potential weaknesses, and practical ways to make it more effective.

Industry partners and the public are asked to only register to speak to one of these categories:

- Government Data Ownership and Protection Requirements
- Prime Contractor Requirements
- Clause Flowdown Requirements
- Other Clause Requirements

To register for the Listening Session in person or virtually, visit: https://gsa.zoomgov.com/webinar/register/4917809414710/WN_2L3o5vduRBOpdur9ub_-0A. Registration will close on Friday, July 3, 2026.

After registering, to request to speak on one of the previously listed categories, do so at <https://forms.gle/1Whv75hUG38ZWtfD7>. This registration will close on Friday, July 3, 2026. Members of the press, in addition to registering for this event, must RSVP to press@gsa.gov no later than Friday, July 3, 2026.

List of Subjects

48 CFR Part 539

Computer technology, Government procurement.

48 CFR Part 552

Government procurement, Reporting and recordkeeping requirements.

Nicholas West,

Director, Office of GSA Acquisition Policy, Integrity & Workforce, Office of Government-wide Policy, Office of Acquisition Policy.

For the reasons set out in the preamble, GSA proposes to amend 48 CFR chapter 5 as follows:

- 1. Add part 539 to read as follows:

PART 539—ACQUISITION OF INFORMATION AND COMMUNICATION TECHNOLOGY

Sec.

539.71 Solicitation provisions and contract clauses.

539.72 [Reserved]

Authority: 40 U.S.C. 121(c).

539.71 Solicitation provisions and contract clauses.

(a) *Basic Safeguarding of Data Within Large Language Model Artificial Intelligence Systems (LLMs)*. The contracting officer must insert the clause at 552.239–7001, *Basic Safeguarding of Data Within Large Language Model Artificial Intelligence Systems*, in solicitations and contracts, including those for commercial products and services, when

Government data will be processed by a LLM.

(b) *Exceptions*. The clause does not apply when—

(1) The LLM is embedded in a common commercial product, such as a word processor or map navigation system (see section 7223(4)(B) of Pub. L. 117–263); or

(2) The LLM functionality is incidental to the primary purpose of the core requirement being procured.

539.72 [Reserved]

PART 552—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

- 2. The authority citation for part 552 continues to read as follows:

Authority: 40 U.S.C. 121(c).

- 3. Add 552.239–7001 to read as follows:

552.239–7001 Basic Safeguarding of Data Within Large Language Model Artificial Intelligence Systems.

As prescribed in 539.71, insert the following clause:

552.239–7001 Basic Safeguarding of Data Within Large Language Model Artificial Intelligence Systems (XXX 2026) (GSAR Deviation)

(a) *Applicability and Flowdown*.

(1) *Applicability*.

(i) This clause applies only when Government Data will be processed by a Large Language Model Artificial Intelligence System (LLM).

(ii) This clause does not apply when—

(A) The LLM is embedded in a common commercial product, such as a word processor or map navigation system (see Section 7223(4)(B) of Public Law 117–263);

(B) The LLM functionality is incidental to the primary purpose of the core requirement being procured.

(2) *Flowdown Requirements*. The Contractor must extend (flowdown) the specific paragraphs of the base clause to any subcontractor or service provider (referred to as “Contractor” in each flowdown supplemental clause) functioning in the applicable roles, as defined in the flowdown supplemental clauses. Where a single entity performs multiple roles, multiple flowdown supplemental clauses should be used:

(i) 552.239–7001–1 LLM Developer Flowdown Requirements (DATE);

(ii) 552.239–7001–2 LLM System Operator Flowdown Requirements (DATE);

(iii) 552.239–7001–3 LLM System Integrator Flowdown Requirements (DATE);

(iv) 552.239–7001–4 LLM Service Provider Flowdown Requirements (DATE).

(b) *Definitions*. As used in this clause—

Background Data means any pre-existing proprietary content, reference materials, knowledge bases, or other intellectual property owned or controlled by the Contractor that may be referenced, retrieved, augmented, or otherwise incorporated into the LLM’s processing or outputs through any enrichment mechanism, including but not limited to retrieval processes, vector stores, embeddings, knowledge graphs, plugins, tool calls, agent actions, or similar mechanisms.

Contractor means the entity that enters into the direct contract with GSA responsible for implementation of this clause (i.e., prime contractor) or, for the purposes of each flowdown supplemental clause, the subcontractor or service provider functioning in the applicable role.

Custom Development means any design of or modifications, customizations, configurations, or enhancements to LLMs or associated implementations or workflows, and any related work product or deliverables, in each case developed specifically for the Government under this contract or task/delivery order, including any modifications, customizations, configurations, or enhancements to LLMs as a result of model training or fine-tuning. Custom Development excludes any background intellectual property (e.g., the underlying supporting services, default configurations, and/or mechanisms) existing prior to entry into this contract or developed independently by the Contractor.

Data has the same meaning as defined in 44 U.S.C. 3502(16) and must, without limiting the generality of the foregoing, specifically include Data Inputs and Data Outputs.

Data Inputs means all data, information, personally identifiable information (PII), or content submitted to the LLM and related operational systems by, or created for, the Government, including but not limited to user prompts, queries, instructions, system prompts, source data, documents, knowledge bases, Government email addresses, user account information, and any other information or content submitted to the LLM and related operational systems by or on behalf of the Government. This definition specifically excludes any background intellectual property or information existing prior to entry into this contract or task/delivery order or

developed independently by such Contractor.

Data Outputs means all data, information, PII, any improvements, enhancements, corrections, annotations, or other modifications made to Data Inputs, or content generated by the LLM in the performance of this contract, including but not limited to responses, results, analyses, anonymized data, derivative data, metadata, logs, synthetic data, and any other output or action produced by the LLM, regardless of whether such output incorporates or is derived from Background Data. This definition specifically excludes technical system-level data that contains no Government information or Government usage context, such as performance metrics, token counts, and processing times.

Government means any entity authorized to obtain procurement services through GSA pursuant to 40 U.S.C. § 501, 502.

Government Data means Data Inputs and Data Outputs.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502(8)).

Large Language Model Artificial Intelligence System (LLM) means a generative artificial intelligence model trained on vast, diverse datasets that enable the model to generate natural-language responses to user prompts (Ref. Executive Order 14319 Section 2). LLM includes the integrated technical and operational environment in which the model is configured, deployed, operated, monitored, or made available for the processing of Government Data, including the model, hosting and access infrastructure, system prompts, configurations, knowledge bases, retrieval mechanisms, Application Programming Interfaces (APIs), user interfaces, guardrails, monitoring systems, and associated workflows.

LLM Developer means the party that performs LLM Development Tasks (as defined in NIST AI RMF 1.0, Appendix A as “AI Development Tasks”) by designing, developing, training, fine-tuning, calibrating, testing, publishing, licensing, or otherwise making available an LLM, including model weights, interfaces, model cards, safety documentation, or conditional usage restrictions. LLM Developer maps primarily to the “AI Development” actor category in NIST AI RMF 1.0, Appendix A.

LLM Service Provider means the party that performs LLM Deployment and Operation & Monitoring (as defined in

NIST AI RMF 1.0, Appendix A as “AI Deployment and Operation & Monitoring”) tasks by providing an LLM-enabled application, product, service, workflow, API, user interface, or business capability to Customers or End Users, and controlling the manner in which the service is presented, accessed, administered, supported, or used within that application or workflow. LLM Service Provider maps primarily to the “AI Deployment” and “Operation and Monitoring” actor categories in NIST AI RMF 1.0, Appendix A.

LLM System Integrator means the party that performs LLM Design and LLM Deployment (as defined in NIST AI RMF 1.0, Appendix A as “AI Design” and “AI Deployment”, respectively) tasks by selecting, configuring, adapting, or materially controlling how an LLM System performs in a specific deployment or use case, including by selecting models, setting system prompts, prompt templates, Retrieval-Augmented Generation (RAG) sources, fine-tuning data, tools, plugins, agents, guardrails, filters, evaluation criteria, human-review thresholds, or output constraints. LLM System Integrator maps primarily to the “AI Design” and “AI Deployment” actor categories in NIST AI RMF 1.0, Appendix A, and includes parties NIST identifies as “system integrators.”

LLM System Operator means the party that performs LLM Deployment and Operation & Monitoring (as defined in NIST AI RMF 1.0, Appendix A as “AI Deployment and Operation & Monitoring”) tasks by hosting, serving, operating, or providing access to an LLM or LLM System, including through cloud infrastructure, model endpoints, runtime environments, API availability, capacity management, logging, retention, and runtime security. LLM System Operator maps primarily to the “AI Deployment” and “Operation and Monitoring” actor categories in NIST AI RMF 1.0, Appendix A, and may also be a “Third-party entity” where it provides such services for another organization.

Material Change means any modification that could affect the trustworthiness, security, or operational integrity of the performance of the contract, especially as they pertain to the processing and protection of Government Data and the contractors involved in that process.

Personally Identifiable Information (PII) has the same meaning as defined in OMB Circular No. A–130.

(c) *Order of Precedence*. For purposes of the order of precedence in GSAR clause 552.212–4, this clause is incorporated into the “schedule of

supplies/services”. This clause establishes specific requirements that take precedence over conflicting provisions in the Contractor’s policies, requirements, terms, conditions, or commercial agreements.

(d) *Contractor Responsibility for LLM*. The Contractor must:

(1) Exercise due diligence in selecting and overseeing the LLM’s Developer(s), System Operator(s), System Integrator(s), and Service Provider(s).

(2) Notify the Contracting Officer, within 72 hours, of any known non-adherence to this clause.

(3) Demonstrate compliance. The Contractor may satisfy due diligence by relying on:

(i) Flowdown of applicable requirements of this clause to LLM’s Developer(s), System Operator(s), System Integrator(s), and Service Provider(s); or

(ii) Obtaining attestation, from an individual with appropriate authority representing the LLM’s Developer(s), System Operator(s), System Integrator(s), and Service Provider(s), that requirements have been implemented.

(e) *Intellectual Property Rights*.

(1) *Rights in Government Data*.

(i) The Government retains full ownership of, and will own, all Government Data and Custom Developments. The Contractor does not have any rights to use Government Data or Custom Developments provided to the Contractor other than those described in paragraph (e)(1)(iii).

(ii) Only LLM Developers, LLM System Operators, LLM System Integrators, and LLM Service Providers may receive and process Government Data.

(iii) The Contractor is granted a limited, revocable, non-exclusive, non-transferable, worldwide, fully paid-up, royalty-free right and license to copy, store, transmit, modify, display, and use Government Data and Custom Developments for the duration of each individual awarded contract or task/delivery order solely for the following permitted purposes:

(A) Performing the specific requirements;

(B) Providing technical support and maintenance as required; and

(C) Providing such other uses as may be expressly authorized in writing by the Contracting Officer.

(iv) To the extent the Contractor obtains any intellectual property rights in Government Data, or any improvements, enhancements, feedback, or derivative works thereof, the Contractor assigns and transfers all such

rights to the Government effective immediately upon creation.

(v) The Contractor retains ownership of the underlying LLM, base models, and Background Data in its original form.

(2) *License Grant to Government.* The Contractor grants to the Government an irrevocable, royalty-free, non-exclusive license to use the LLM for the duration of the work defined in the contract or task/delivery order. This license is strictly limited to the specific purposes and scope of work defined within the contract or task/delivery order, and is restricted to the commercially available features, Background Data, and functionality of the LLM as described in and necessary to fulfill this contract or task/delivery order and its accompanying documentation, unless specified otherwise. This license includes the right to:

(i) Operate and access the LLM through agreed-upon methods;

(ii) Allow authorized Government personnel and contractors to use the LLM; and

(iii) Integrate the LLM with Government systems as necessary.

(3) *Prohibited Uses of Government Data. Use of Government data is limited per paragraph (e)(1)(iii).* Other uses of Government data are prohibited. Examples of prohibited use of Government Data includes:

(i) Training, fine-tuning, or otherwise improving an LLM, including those operated by third parties, or to develop or improve the LLM(s) for any other customers or any commercial or non-commercial purposes.

(ii) Using Government Data to inform the Contractor's advertising, marketing, sales, monetization, strategy, operations, or other business decisions, or to provide to other Government or non-Government entities.

(iii) Retaining, accessing, or using beyond the scope and duration expressly permitted in the contract.

(iv) Processing or storing Government Data with, or transferring Government Data to, any party not authorized under this contract or task/delivery order or without appropriate extension (flowdown) of applicable requirements.

(v) Selling or licensing Government Data to any party.

(4) *Government Data Handling and Processing Requirements.* Unless otherwise expressly authorized by the Contracting Officer:

(i) The Contractor must implement reasonable technical, administrative, physical, and organizational safeguards to protect Government Data from loss, damage, destruction, unauthorized alteration, or corruption, and prevent its

unauthorized, accidental, or unlawful access, disclosure, use, or processing;

(ii) The Contractor must implement Data Handling Procedures that restrict human access to Government Data. These protocols must be implemented at the contract level and customization at the individual contract or task/delivery order level. Automated processing systems and operational controls that prevent human personnel from the Contractor or any Third-party entity from viewing, accessing, or reviewing Government Data during normal operations include:

(A) Automated data ingestion, processing, and response generation without human content review;

(B) Technical access controls that prevent personnel from viewing Government Data;

(C) Encrypted data transmission and processing that renders Government Data unreadable to human personnel;

(D) Administrative and technical safeguards that allow system operation, monitoring, and maintenance without exposing Government Data content; and

(E) Audit logging systems that track data processing activities without capturing or displaying actual Government Data.

(iii) The Contractor must ensure Government Data is stored or processed only when reasonably necessary for the performance of the contract;

(iv) The Contractor must provide tools that enable the Government to maintain detailed records of all processing activities involving Government Data;

(v) The Contractor must comply with the following Data localization requirements, including but not limited to:

(A) Not removing or allowing removal of any such Government Data from the agreed-upon premises or FedRAMP-authorized services, without express written consent from the Contracting Officer; and

(B) Not transmitting, storing, taking, or accessing such Government Data, or allowing such Government Data to be transmitted, stored, taken, or accessed by any means outside of the agreed-upon premises or authorized services, without express written consent from the Contracting Officer.

(vi) The Contractor must implement and maintain appropriate technical and organizational measures to ensure that all such Government Data is logically segregated from the Data of any non-Government customer or client, and is not commingled with Data of other customers or clients and provides adequate defense in depth through access controls, policy enforcement points, labeling, and/or encryption

mechanisms and must perform continuous monitoring to protect against unauthorized access by external and internal threat actors, third parties, or disclosure resulting from human or machine error. Logical segregation does not require physical or dedicated instances within contractor-hosted or controlled systems, continuing compliance with the specified FedRAMP authorization level is deemed to satisfy these requirements by achieving equivalent security and separation.

(vii) Upon completion, termination or expiration of the contract or task/delivery order, unless otherwise directed in writing by the Contracting Officer, the Contractor must securely and permanently delete all such Government Data and any Custom Developments from the LLM and all its other systems and all copies, backups and derivatives thereof, and certify deletion to the Contracting Officer in writing.

(viii) *Custom Developments and Model Rights.* If there is a requirement for custom developments, the Contractor must:

(A) Dedicate the Custom Developments, including any customized or enhanced models resulting from such Custom Developments, to the Government's exclusive use;

(B) Treat such Custom Developments, custom models, and all associated Data as the Government's confidential information; and

(C) Not use, reproduce, or derive benefit from such Custom Developments or custom models for any other purpose, or for the benefit of any other party, without express written authorization from the Contracting Officer.

(ix) *Feedback.* The Government retains ownership of all feedback provided by the Government to the Contractor with respect to the LLM or Custom Developments, regardless of whether such feedback is generated by Government personnel, the Contractor, or through automated processes. If feedback includes Government Data and Government confidential information, that feedback may not be used for system improvement purposes or any other purposes (except solely in the performance of this contract).

(f) *Contractor Obligations for Compliance, Reporting, and Documentation.* The Contractor must:

(1) Disclose all LLMs used or made available in performance of this contract or a task/delivery order. Disclose all entities filling the roles defined by the flowdown supplemental clauses. Disclosures are due to the Contracting

Officer or ordering Contracting Officer by the date specified in the contract or task/delivery order. If no date is specified, disclosures are due within 120 days after commencing work under the contract or task/delivery order.

(2) Maximize the use of LLMs that meet the following criteria:

(i) Controlling Entity & Jurisdiction: Each LLM is developed, managed, and operated by an entity that is incorporated in the United States (U.S.) and is subject to U.S. law and jurisdiction.

(ii) Protection Against Foreign Compulsion:

(A) Each LLM's performance, operations, or protections cannot be controlled by a foreign Government.

(B) No foreign Government or entity can compel disclosure of Government Data, or operational details that could compromise each LLM's integrity or security.

(C) Each LLM, and any components performing core model, data storage or processing, output generation, or security functions, are prohibited from being developed, managed, or operated by entities subject to the direction, influence, or control of adversary foreign governments (see 15 CFR 791.4).

(iii) Component Flexibility & Risk Mitigation: Incidental foreign-developed components (e.g., open-source components, published research), ancillary Third-party services, or globally operated infrastructure dependencies are permissible, provided:

(A) They do not introduce security risks or foreign control that would violate criteria (f)(2)(i) or (f)(2)(ii).

(B) The systems storing or processing Government Data satisfy applicable Federal security requirements, including those for data residency and isolation.

(C) A risk-based approach is applied, focusing on objective criteria such as ownership, control, hosting, and security posture.

(3) Disclose whether the LLM has been modified or configured to comply with any non-U.S. federal government statutes, regulations, or policies no later than thirty (30) days after award to the Contracting Officer, unless otherwise stated in the solicitation, contract, or task/delivery order.

(4) Provide a means for the Government to implement human oversight, intervention, and traceability. If the LLM uses intermediary processing such as reasoning, retrieval, or agentic processes, the LLM must summarize intermediary steps from data input to data output, and make this information accessible through data output, audit trail, and as applicable the user

interface. At minimum, the LLM must include:

(i) Summarized intermediate processing actions and decision points;

(ii) Model routing decisions with accompanying rationale; and

(iii) Data retrieval methods employed (e.g., Retrieval-Augmented Generation (RAG), web search), including complete source attribution with direct links and relevant excerpts from materials used in response generation.

(5) Notify the Contracting Officer and any Government provided point of contacts as soon as possible but not longer than within 72 hours of the discovery of any incident (as defined by the Federal Information Security Modernization Act of 2014 in 44 U.S.C. 3552(b)(2)) affecting any contractors, including Third-party entities, handling Government Data and provide daily status updates to all points of contact until resolved.

(i) Such notification must include, to the extent known at the time:

(A) Nature and scope of the incident;

(B) Data potentially affected;

(C) Immediate remediation steps taken;

(D) Timeline for full resolution; and

(E) Measures to prevent recurrence.

(ii) Where FedRAMP incident communication and response procedures conflict with contractual requirements, the FedRAMP procedures take priority if the system is required to be FedRAMP Authorized.

(iii) The Contractor must preserve all relevant logs, forensic images, and incident artifacts for a minimum of 90 calendar days from a security incident involving Government Data to support follow-on investigation activity by law enforcement entities.

(iv) The Contractor must also complete the CISA incident reporting form (<https://myservices.cisa.gov/irf>).

(6) Establish feedback mechanisms (consistent with OMB M-25-21 and successor requirements) allowing the Government to:

(i) Provide performance feedback and improvement requests through formal channels;

(ii) Request system modifications or enhancements; and

(iii) Report operational concerns without requiring incident classification.

(7) Provide, upon Government request, and under appropriate confidentiality protections, existing commercial documentation or disclosures sufficient to demonstrate compliance, including but not limited to:

(i) Verification of compliance with this clause and the contract;

(ii) List of entities involved in performance of this contract or task/delivery order, the entities' role(s), as defined by the flowdown supplemental clauses, which requirements of this clause are applicable to each entity, and the entities' approach to addressing the requirements in this clause;

(iii) LLM decision-making processes, logic, and operational parameters;

(iv) LLM Developers, general model characteristics, intended use, limitations, and risk considerations to enable informed and responsible use by the Government. The contractor is not required to disclose proprietary source code, model weights, or trade secrets.

(v) System documentation consistent with NIST AI Risk Management Framework guidelines, Unbiased AI Principles, and LLM Transparency requirements such as system cards or equivalent documentation.

(vi) *Transparency & Auditability*: The Contractor must provide commercially available means for the Government to implement appropriate human oversight, intervention, and traceability for the contracted use case, and to understand the role of various components in generating responses, to the extent commercially available and technically feasible;

(vii) Privacy controls effectiveness and PII processing prohibition compliance;

(viii) Testing methodologies used to detect and mitigate noncompliance with the unbiased AI principles described in paragraph (j)(1);

(ix) Known biases (including commercial, political, or personal considerations, advertising, endorsements, or fraudulent/corrupt interests), limitations, truthfulness concerns, and performance metrics;

(x) Influence, direction, or control of an adversary foreign governments (see 15 CFR 791.4);

(xi) FedRAMP authorization packages, continuous monitoring data, and assessment artifacts necessary to issue or maintain an authorization to operate, consistent with 44 U.S.C. 3609(a)(8) and OMB M-24-15 and successor requirements; and

(xii) Any other information necessary for the Government to monitor and evaluate the LLM's performance, risks, and effectiveness and to complete an LLM Impact Assessment required by OMB M-25-21 and successor requirements.

(g) *Privacy and Confidentiality Protections*.

(1) To the extent the Contractor has available tools, they must provide tools to enable the Government to implement appropriate Government-configurable

controls, including but not limited to automated detection mechanisms and clear user notifications to manage, prevent, and reject the entry or persistence of PII within the LLM.

(2) The Government, absent specific legal requirements, will not disclose confidential documentation or information provided by the Contractor.

(h) *Data Portability and Interoperability.* The Contractor must:

(1) Provide and ensure that LLM services support the export of Government Data (including but not limited to: user-generated content, interaction history, uploaded content and media, and knowledge bases) in open or standard machine-readable formats, together with sufficient associated metadata and schema information necessary for the Government to retrieve, use, or migrate Government Data to another service.

(2) Provide and support documented APIs sufficient for Government integration and data export to the extent the service uses APIs.

(3) Not impose proprietary formats, technical restrictions, additional costs, or additional licensing conditions that materially impair the Government's ability to retrieve, use, or migrate Government Data to another service.

(4) Provide tooling or interfaces to facilitate migration of Government Data and Custom Developments in a secure manner.

(i) *Change Notification.*

(1) Advance Notice of Material Changes. The Contractor must provide written notice to the Contracting Officer at least thirty (30) calendar days prior to any planned material change affecting the services provided under this contract, including:

(i) Adding, replacing, or materially changing any LLMs, LLM's Developer(s), System Operator(s), System Integrator(s), or Service Provider(s);

(ii) Changes to the services handling Government Data, including discontinuation or material reduction of data protection controls applied to Government Data, or change in FedRAMP Authorization Status; or

(iii) Any modification, configuration, or training change to the LLM made to comply with any non-U.S. government statute, regulation, or policy.

(2) Model Version Changes. The Contractor must use reasonable efforts to provide the Government with concurrent access to any successor LLM, and associated documentation, for a minimum evaluation period of thirty (30) calendar days for major versions, and fifteen (15) calendar days for minor versions, prior to discontinuing or

replacing any LLM in use under this contract.

(3) Safety and Performance Degradation. The Contractor must notify the Contracting Officer within seven (7) calendar days of identifying any change that materially increases output bias; decreases safety guardrails or behavioral constraints; or degrades performance or truthfulness of outputs. The notification must describe the change, its purpose, the evaluation approach used and any new limitations, trade-offs, or potential negative impacts identified.

(4) Emergency and Unplanned Changes. If the Contractor implements a change without providing sufficient advance notice, or if a change is necessitated by a security or service emergency, the Contractor must:

(i) Notify the Contracting Officer as soon as practicable upon learning of the change; and

(ii) Describe any remediation or rollback actions available.

(5) *Notification:* All notifications under paragraph (i) must include, to the extent known at the time of notification:

(i) Description of change;

(ii) Affected roles, services, systems, and Government Data;

(iii) Any limitations, trade-offs, or negative impacts;

(iv) Evaluation approach used to assess the change;

(v) Any remediations or rollback actions; and

(vi) Confirmation of applicable requirements of this clause have been flowed down appropriately.

(j) *Performance, Evaluation, and Remediation.*

(1) *Unbiased AI principles.* The Contractor must ensure the LLM is developed and monitored in accordance with the following unbiased AI principles:

(i) The LLM must be truthful in responding to user prompts seeking factual information or analysis. The LLM must prioritize historical accuracy, scientific inquiry, and objectivity and must acknowledge uncertainty where reliable information is incomplete or contradictory.

(ii) The LLM must be a neutral, nonpartisan tool that does not manipulate responses in favor of ideological dogmas. The Contractor must not intentionally introduce or embed partisan or ideological judgments into the LLM's Data Outputs through methods such as training data selection, fine-tuning, Retrieval-Augmented Generation (RAG) references, system prompts, or other configuration methods.

(iii) The Contractor must implement continuous improvement processes to

enhance detection and mitigation of performance, trustworthiness, bias, and/or systems generating illegal or prohibited content, including regular evaluation of system outputs (excluding Data Outputs) against verified factual sources.

(2) *Government Evaluation Rights and Remediation.*

(i) The Government reserves the right to conduct automated assessments of the LLM, as deployed and configured for government users, at any time using its own benchmarks. These evaluations may assess bias, truthfulness, safety, unsolicited ideological content, and other factors determined by the Government in order to facilitate evaluations.

(ii) The Contractor must provide tools and interfaces that enable the Government to run its benchmarks in an automated fashion to test the production LLM and identify any material gaps.

(iii) The Government may provide such results to the Contractor to support remediation efforts.

(iv) All benchmarks, test data, and methodologies developed or used by the Government for such assessments are considered Government Data. The Government is under no obligation to disclose or provide access to the underlying data, methodologies, or systems, with the exception of data or methodologies used as the basis for an adverse action under paragraph (j)(3)(ii).

(3) *Non-Compliance.*

(i) The Government retains the right to suspend use of the LLM until performance issues are satisfactorily addressed;

(ii) The Contractor is liable for reasonable decommissioning costs if the Contracting Officer terminates this contract or task/delivery order for cause for failure to remediate after receiving specific written notice of non-compliance from the Contracting Officer with the Unbiased AI Principles described in paragraph (j)(1).

(A) Decommissioning cost liability are not to exceed ____ [Contracting Officer to insert a percentage] at a percentage of contract value; and

(B) The Government must disclose information, under appropriate confidentiality protections, to enable the Contractor to understand the basis for the Government's determination and take reasonable remediation actions.

(end of clause)

■ 4. Add 552.239-7001-1 to read as follows:

552.239-7001-1 LLM Developer Flowdown Requirements.

As prescribed in 552.239-7001(a)(2), use the clause at 552.239-7001-1, LLM

Developer Flowdown Requirements (DATE), to extend (flowdown) these requirements to a LLM Developer (*e.g.*, model architecture, training, weights, model cards, safety documentation, base capabilities, acceptable use policies, base safety filters), as defined in clause 552.239–7001(b).

Basic Safeguarding of the Data Within Large Language Model Artificial Intelligence Systems—LLM Developer Flow-Down Requirements (DATE)

- (a) Applicability
 - (b) Definitions
 - (e) Intellectual Property Rights
 - (f) Contractor Obligations for Compliance, Reporting, and Documentation
 - (g) Privacy and Confidentiality Protections
 - (i) Change Notification
 - (j) Performance, Evaluation, and Remediation
- (end of clause)

■ 5. Add 552.239–7001–2 to read as follows:

552.239–7001–2 LLM System Operator Flowdown Requirements.

As prescribed in 552.239–7001(a)(2), use the clause at 552.239–7001–2, LLM System Operator Flow-Down Requirements (DATE), to extend (flowdown) these requirements to a LLM System Operator (*e.g.*, cloud infrastructure, model hosting, endpoints, API availability, runtime security, logging, retention, data residency, capacity management, rate limits), as defined in clause 552.239–7001(b).

Basic Safeguarding of the Data Within Large Language Model Artificial Intelligence Systems—LLM System Operator Flow-Down Requirements (DATE)

- (a) Applicability
- (b) Definitions

(e) Intellectual Property Rights

The following subparagraphs from paragraph (f) Contractor Obligations for Compliance, Reporting, and Documentation

(f)(2), (f)(2)(iii)(B)

(f)(4)

(f)(5)

(f)(6)

(f)(7)

(g) Privacy and Confidentiality Protections

(h) Data Portability and Interoperability

The following subparagraphs from

paragraph (i) Change Notification

(i)(1)(i), (i)(1)(ii)

(i)(3)

(i)(4)

(i)(5)

(j) Performance, Evaluation, and Remediation

(end of clause)

■ 6. Add 552.239–7001–3 to read as follows:

552.239–7001–3 LLM System Integrator Flowdown Requirements.

As prescribed in 552.239–7001(a)(2), use the clause at 552.239–7001–3, LLM System Integrator Flow-Down Requirements (DATE), to extend (flowdown) these requirements to a LLM System Integrator (*e.g.*, model selection, system prompts, prompt templates, RAG sources, vector stores, tools, plugins, agents, guardrails, filters, fine-tuning data, evaluation criteria, human-review thresholds, output constraints, workflow logic), as defined in clause 552.239–7001(b).

Basic Safeguarding of the Data Within Large Language Model Artificial Intelligence Systems—LLM System Integrator Flow-Down Requirements (DATE)

- (a) Applicability
- (b) Definitions
- (e) Intellectual Property Rights

(f) Contractor Obligations for Compliance, Reporting, and Documentation

(g) Privacy and Confidentiality Protection

(h) Data Portability and Interoperability

The following subparagraphs from

paragraph (i) Change Notification

(i)(1)(i), (i)(1)(iii)

(i)(2)

(i)(3)

(i)(5)

(j) Performance, Evaluation, and Remediation

(end of clause)

■ 7. Add 552.239–7001–4 to read as follows:

552.239–7001–4 LLM Service Provider Flowdown Requirements.

As prescribed in 552.239–7001(a)(2), use the clause at 552.239–7001–4, LLM Service Provider Flow-Down Requirements (DATE), to extend (flowdown) these requirements to a LLM Service Provider, as defined in clause 552.239–7001(b).

Basic Safeguarding of Data Within Large Language Model Artificial Intelligence Systems—LLM Service Provider Flow-Down Requirements (DATE)

- (a) Applicability
 - (b) Definitions
 - (e) Intellectual Property Rights
 - (f) Contractor Obligations for Compliance, Reporting, and Documentation
 - (g) Privacy and Confidentiality Protections
 - (h) Data Portability and Interoperability
 - (i) Change Notification
 - (j) Performance, Evaluation, and Remediation
- (end of clause)

[FR Doc. 2026–12205 Filed 6–16–26; 8:45 am]

BILLING CODE 6820–61–P



April 2026

ARTIFICIAL INTELLIGENCE ACQUISITIONS

Agencies Should
Collect and Apply
Lessons Learned to
Improve Future
Procurements



Agencies Should Collect and Apply Lessons Learned to Improve Future Procurements

GAO-26-107859

April 2026

A report to congressional requesters

For more information, contact: William Russell at RussellW@gao.gov or Candice N. Wright at WrightC@gao.gov.

What GAO Found

Federal agencies reportedly more than doubled their use of artificial intelligence (AI) from 2023 to 2024, and they used a range of approaches to acquire additional AI capabilities through fiscal year 2025. GAO identified trade-offs facing agencies as they acquire AI, and some associated challenges and benefits. For example:

- **Agency-directed vs. vendor-driven approaches.** Some agencies awarded new contracts in pursuit of AI solutions. In other instances, industry introduced capabilities to agencies in the absence of specific AI requirements.
- **Contracts vs. other agreements.** Agencies used different types of contracts to acquire AI capabilities. In some instances, agencies also leveraged other agreements not governed by federal acquisition regulations to develop more advanced AI capabilities.
- **AI as a service vs. a product.** Some agencies bought AI as a product, such as software. However, agency officials told GAO they acquire AI as a service where the vendor provides AI capabilities and outputs on an ongoing basis.

GAO identified several strategic and programmatic challenges agencies faced when acquiring AI capabilities.

Key Procurement Challenge Areas Identified by Selected Agencies

Strategic	Programmatic
Access to subject matter experts	Requirements definition and contract terms
Protections for government data and intellectual property rights	Early testing and continuous evaluation
Traditional acquisition timeframes and contract approaches	Artificial intelligence pricing and overall cost

Source: GAO analysis of interviews with agency officials from the General Services Administration and Departments of Commerce, Defense, Homeland Security, and Veterans Affairs. | GAO-26-107859

In April 2025, the Office of Management and Budget (OMB) issued guidance to help agencies acquire AI responsibly. OMB directed agencies to update their AI policies to comply with OMB's requirements. GAO previously reported that agency-level implementation is critical to achieving acquisition goals directed by OMB ([GAO-25-107398](#)).

In this review, GAO found the selected agencies were not yet systematically collecting lessons learned from AI acquisitions—a necessary first step to share knowledge about AI acquisitions in accordance with OMB guidance. OMB has stated that agencies should share knowledge about AI acquisitions through a web-based repository developed by the General Services Administration (GSA). However, officials at four agencies—GSA and the Departments of Defense (DOD), Homeland Security (DHS), and Veterans Affairs (VA)—told GAO they were not prepared to do so because their agency policies did not require them to collect lessons learned. As a result, the agencies are missing opportunities to identify and apply best practices—such as contract terms related to data rights or testing requirements—or to avoid mistakes as agencies increasingly acquire AI.

Why GAO Did This Study

Industry leads AI development, reportedly investing over \$250 billion in 2024 alone. Federal agencies are finding many opportunities to use AI to execute their missions. They already use AI for veteran services, enhancements to weapon systems, and administrative tasks. To realize the benefits of AI, federal agencies often contract with companies to acquire solutions. Members of Congress and others have raised concerns about federal AI acquisitions. These concerns include long-standing acquisition issues, such as fostering competition, as well as issues specific to AI, such as training AI models on flawed data.

GAO was asked to review federal AI acquisitions. This report addresses (1) acquisition approaches agencies are using to adopt AI, (2) types of challenges agencies face when acquiring AI capabilities, and (3) the extent to which selected agencies are prepared to share knowledge related to acquiring AI solutions.

GAO conducted in-depth reviews of 13 AI acquisitions at four federal agencies—DOD, DHS, GSA, and VA. GAO selected these agencies based on maturity of AI acquisition efforts and approaches to acquiring AI capabilities, among other factors. GAO reviewed the agencies' relevant policies, and interviewed senior AI acquisition leaders at the selected agencies. GAO also analyzed OMB guidance.

What GAO Recommends

GAO is making a total of four recommendations. Specifically, GAO is recommending that DOD, DHS, GSA, and VA update their policies to require officials to systematically collect lessons learned from AI acquisitions to enable sharing and application by other agencies. The agencies concurred with all of the recommendations.

Contents

Letter		1
	Background	4
	As AI Technology Rapidly Evolves, Agencies Are Using a Wide Range of Acquisition Approaches	16
	Agencies Face Strategic and Programmatic Challenges When Acquiring AI Capabilities	22
	Knowledge Sharing Can Help Agencies Apply Lessons Learned	28
	Conclusions	31
	Recommendations for Executive Action	31
	Agency Comments	32
Appendix I	Sample of 13 AI Acquisitions from Selected Agencies	34
Appendix II	Comments from the Department of Defense	35
Appendix III	Comments from the Department of Homeland Security	37
Appendix IV	Comments from the General Services Administration	40
Appendix V	Comments from the Department of Veterans Affairs	41
Appendix VI	GAO Contacts and Staff Acknowledgments	44
Tables		
	Table 1: Required or Recommended Agency Actions in OMB Guidance When Acquiring AI	15
	Table 2: Key Procurement Challenge Areas Identified by Selected Agencies	22
	Table 3: Lessons Learned Related to Key Artificial Intelligence (AI) Acquisition Challenges	29
	Table 4: GAO Sample of 13 AI Acquisitions from Selected Agencies	34

Figures

Figure 1: Selected Types of Artificial Intelligence Capabilities	6
Figure 2: Phases of the Artificial Intelligence (AI) Development Life Cycle	7
Figure 3: Timeline of Key Artificial Intelligence Legislative and Executive Guidance	14
Figure 4: Selected Federal Government AI Solutions	17

Abbreviations

AI	artificial intelligence
DOD	Department of Defense
DHS	Department of Homeland Security
EO	executive order
FAR	Federal Acquisition Regulation
FEMA	Federal Emergency Management Agency
GSA	General Services Administration
IDIQ	indefinite delivery/indefinite quantity
IP	intellectual property
NGA	National Geospatial-Intelligence Agency
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OTA	other transaction agreement
VA	Department of Veterans Affairs

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



April 13, 2026

The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Thom Tillis
Chairman
Subcommittee on Intellectual Property
Committee on the Judiciary
United States Senate

Federal agencies are finding many opportunities to use artificial intelligence (AI) to improve how they execute their missions. They are already using AI to try to improve the services provided to veterans, enhance the effectiveness of weapon systems, and increase the efficiency of administrative activities, to name a few examples. To this end, agencies are engaging the private sector to acquire an array of AI solutions, including models, the infrastructure necessary for those models, and the systems that use AI model outputs.¹

While often supportive of the promise AI offers, members of Congress and others have raised concerns about the federal government's acquisition of AI solutions, particularly in the current landscape where AI capabilities, markets, and federal policy are rapidly evolving. Some of these concerns involve long-standing acquisition challenges, such as monitoring performance, obtaining necessary data rights, and increasing opportunities for competition. Other concerns are unique to acquiring AI solutions, including concerns that vendors may be training their models on flawed data, and that model performance may degrade over time, leading to unreliable outputs. To help agencies improve how they are acquiring AI capabilities, in April 2025, the Office of Management and Budget (OMB) issued Memorandum M-25-22, *Driving Efficient Acquisition of Artificial Intelligence in Government*.²

¹For the purposes of this report, we use "model" to refer to the result of an algorithm "trained" on a set of data.

²Office of Management and Budget, *Driving Efficient Acquisition of Artificial Intelligence in Government*, OMB Memorandum M-25-22 (Washington, D.C.: Apr. 3, 2025).

You asked us to review federal AI acquisitions. This report addresses (1) acquisition approaches agencies are using to adopt AI, (2) types of challenges that agencies face when acquiring AI capabilities, and (3) the extent to which selected agencies are prepared to share knowledge related to acquiring AI solutions.

To identify acquisition approaches agencies are using to adopt AI capabilities, we reviewed AI activities at the Departments of Commerce (Commerce), Defense (DOD), Homeland Security (DHS), and Veterans Affairs (VA); and the General Services Administration (GSA). Our review of Commerce's activities focused primarily on government-wide initiatives led by the National Institute of Standards and Technology (NIST) and senior acquisition leaders, rather than specific AI solutions. We selected these agencies to account for relatively mature AI acquisition efforts (DHS and DOD), a large number of "high-impact" AI solutions (DHS and VA), and AI acquisition responsibilities spanning the federal government (GSA and Commerce).³ We reviewed the agencies' AI policies and interviewed senior acquisition leadership to understand the agencies' AI acquisition processes.

For our purposes, we considered agencies' AI solutions to be acquisitions based on agencies' use of contracts—which we reviewed—to pay for AI products, services, license agreements, development support, or testing. We selected a nongeneralizable sample of 13 AI acquisitions from DOD, DHS, GSA, and VA for in-depth review to cover a range of factors, including: a) impact on citizens (e.g., affecting agency decisions about allocation of benefits); b) different types of AI capabilities, such as machine learning or computer vision; c) how the AI solution was acquired, i.e., commercially available or custom development; d) different acquisition phases (starting with developmental contract awards through the end of the program life cycle); e) different contract types, such as firm-fixed price; and f) "high-impact" AI solutions. We selected solutions to achieve a mix of examples that account for variation across these factors.

To select the nongeneralizable sample of AI acquisitions, we used a multifaceted approach. For civilian agencies, we reviewed publicly available AI use case inventories found on each agency's website, as well

³The Office of Management and Budget (OMB) defines "high-impact" as when AI output serves as a principal basis for decisions or actions that have a legal, material, binding, or significant effect on certain interests, including an individual's civil rights and human safety. See *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust*, OMB Memorandum M-25-21 (Washington, D.C.: Apr. 3, 2025).

as OMB's consolidated AI use case inventory from December 2024, which was the most complete data at the start of our review. We also reviewed news sources for AI use cases that matched our selection factors. We then coordinated with knowledgeable agency officials to determine if potential use cases we identified in the public inventories and news sources were correctly categorized as having an affiliated contract. In one case, agency leadership suggested a recent AI use case that was not in public inventory. Based on these steps, we selected four use cases with associated contracts from DHS, two from GSA, and three from VA. To identify potential DOD use cases, we coordinated with officials from the Office of the Under Secretary of Defense for Acquisition and Sustainment and the Chief Digital and Artificial Intelligence Office to review a classified list of over 200 AI-related activities at DOD.⁴ Using our selection factors outlined above, we selected four solutions with associated contracts or agreements to include in our in-depth review.

From our sample of AI acquisitions, we analyzed 44 contracts and agreements awarded between September 2018 and February 2025 and supporting program documentation. In addition, we interviewed officials directly supporting the sample of AI acquisitions to understand the contract mechanisms and acquisition approaches they used to acquire AI solutions. For a full list of the AI acquisitions we reviewed in-depth, see appendix I. We also reviewed highly publicized AI acquisition approaches announced in fiscal year 2025 to a lesser extent.

To determine the types of challenges that agencies face when acquiring AI solutions, we first interviewed officials at our five selected agencies, including agency leadership and staff supporting our sample of AI acquisitions. Among the challenges agency officials shared with us, we selected those identified by the majority of our five selected agencies and then grouped the most commonly cited issues into six challenge areas. We then verified that these challenges were issues across all five of our selected agencies. We reviewed OMB's government-wide AI acquisition guidance, M-25-22, to identify steps in the guidance that corresponded to the challenges raised by officials at our five selected agencies. Specifically, we compared the required and recommended actions for agencies in that policy to the challenges identified through interviews with

⁴DOD is not required to maintain and publish an AI use case inventory as most executive branch agencies are required to do. However, the department is taking some steps to identify and maintain insight into AI activities across the department.

senior acquisition leadership from our selected agencies and officials from our nongeneralizable sample of AI acquisitions.

To assess the extent to which selected agencies are prepared to share knowledge about AI acquisitions as directed by the recent OMB guidance, we assessed requirements in M-25-22 and interviewed senior acquisition leaders and officials from our nongeneralizable sample about how, if at all, they documented lessons learned. We also conducted targeted reviews of relevant departmental or agency-specific AI policies to corroborate certain statements from these officials.

We conducted this performance audit from October 2024 to April 2026 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings based on our audit objectives.

Background

The term AI applies to a broad array of algorithms and techniques that enable computer systems to make predictions, learn concepts or tasks, and solve complex problems in a manner that mimics human intelligence.⁵ Recently, industry-driven AI advances have rapidly enabled a wide variety of new capabilities with real-world applications that can support federal agencies' missions. To help agencies realize the benefits of these recent advances, Congress and the Executive Branch have taken steps to improve federal AI acquisitions, including establishing guidance to help agencies better acquire AI.

Industry-led Evolution of AI Technologies

Key AI concepts, such as computer programming and algorithms, date back to well beyond the 1950s when modern computing took hold. More recently, AI capabilities and their respective markets have evolved at a rapid pace. Industry has spent billions of dollars to support the development and refinement of AI models over the last decade. The Stanford University Institute for Human-Centered AI reported that the private sector leads AI development, with nearly 90 percent of notable models—those deemed as particularly influential models within the AI ecosystem—originating from industry in 2024 compared to 60 percent in

⁵GAO, *Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon Systems*, [GAO-22-104765](#) (Washington, D.C.: Feb. 17, 2022); and *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities*, [GAO-21-519SP](#) (Washington, D.C.: June 30, 2021).

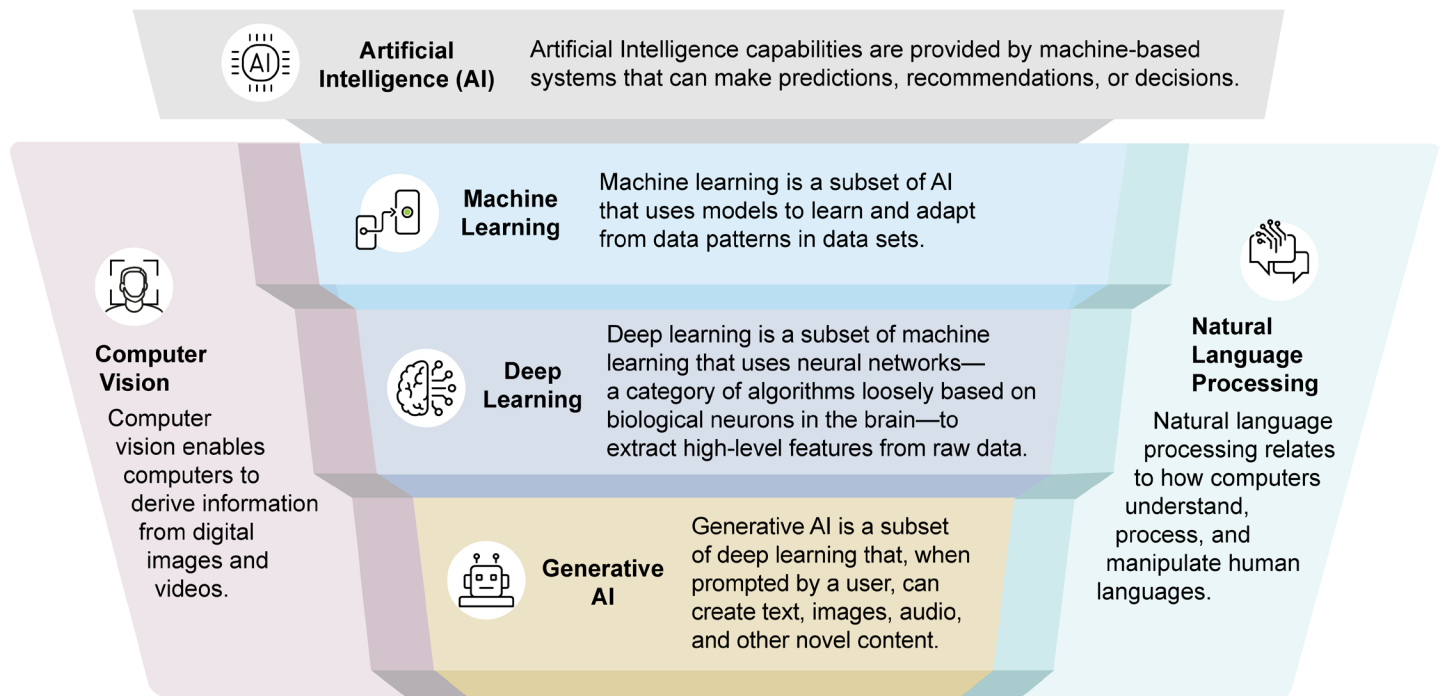
2023.⁶ Those researchers also found that corporate AI investment reached over \$250 billion in 2024 alone. They also found that, over the past decade, the AI sector has experienced dramatic expansion, with total investment growing more than thirteenfold since 2014. As a result, the sophistication of AI models has shifted from conventional AI systems that classify or predict to generative and frontier models capable of enabling a wide variety of real-world applications. For example, AI capabilities underpin online tax preparation services and facial recognition systems. More advanced AI systems, such as generative AI models, can create multimodal content, such as text, images, audio, and video.

Types of AI Capabilities

Within the field of AI, there are various capability types such as machine learning and deep learning that introduce more complex types of models. In addition, there are specific capabilities that overlap these fields. For example, computer vision enables computers to derive information from digital images and videos, whereas natural language processing enables computers to understand, manipulate, and process human language. Figure 1 provides more details about the capabilities that we reviewed in our sample of AI acquisitions.

⁶Nestor Maslej, et al, "The AI Index 2025 Annual Report," AI Index Steering Committee, Institute for Human-Centered AI, (Stanford, CA: Stanford University, April 2025).

Figure 1: Selected Types of Artificial Intelligence Capabilities



Source: GAO analysis of Congressional Research Service documentation; stock.adobe.com/iierlok_xolms (icons) and GAO (Computer Vision icon). | GAO-26-107859

AI Development Life Cycle The development life cycle of an AI system can be categorized into four phases that account for continuous learning: design, development, deployment, and continuous monitoring. These phases are often iterative and not necessarily sequential (see fig. 2).

Figure 2: Phases of the Artificial Intelligence (AI) Development Life Cycle



Source: GAO. | GAO-26-107859

Data and Computing Needs for AI

We have previously reported on the role that data play in developing AI capabilities, as machine learning systems begin with data—generally in large amounts—and infer rules or decision procedures that aim to predict

specified outcomes.⁷ High quality data are critical for training, testing, and validating AI systems before and after deployment to ensure AI systems produce consistent and accurate results.⁸ AI systems based on machine learning models learn from data, known as training sets, in order to perform a task. A testing set is a subset of the data used to test the trained model. The testing set should be large enough to yield statistically relevant results and be representative of the data set as a whole.

Computing requirements also play a key role in developing AI capabilities. To process vast volumes of data, AI systems often require considerable computing power and new architecture, often cloud-based, to support model training and development. Stanford University researchers found that the training computing power (also known as compute) for notable AI models doubles approximately every 5 months.⁹ New academic research shows that large-scale industry investment drives these model scaling and performance gains. We have reported that major AI breakthroughs that have occurred in the past decade in computing power and data availability were needed to develop advanced AI models.¹⁰

Federal Contracting

Federal agencies rely on the private sector to deliver goods and services that help agencies perform their missions, typically using contracts to acquire software, cutting edge technologies, and commercial products and services. AI can fall into all three of these categories.

The federal acquisition life cycle can be categorized into three general contracting phases: pre-award, award, and post-award.

- Pre-award phase activities often include defining requirements, acquisition planning, and preparing the solicitation.
- Award phase activities often involve the evaluation of offers, price negotiations and discussions with offerors, and the selection of awardees.

⁷[GAO-21-519SP](#).

⁸[GAO-21-519SP](#).

⁹Nestor Maslej, et al, "The AI Index 2025 Annual Report," AI Index Steering Committee, Institute for Human-Centered AI, (Stanford, CA: Stanford University, April 2025).

¹⁰GAO, *Artificial Intelligence: Generative AI Technologies and Their Commercial Applications*, [GAO-24-106946](#) (Washington, D.C.: June 20, 2024).

-
- Post-award phase activities often involve agency oversight of contractor performance—which includes continuous monitoring—and contract administration and closeout.

Agencies typically follow the Federal Acquisition Regulation (FAR) and agency supplements to award contracts.¹¹ The FAR provides agencies with a broad range of contract types and vehicles to acquire products and services. These include leveraging established government-wide or agency-wide multiple-award indefinite delivery/ indefinite quantity (IDIQ) contracts or developing custom solutions by entering into a contract with one vendor using a variety of contract types, such as fixed-price, cost-reimbursement, or single award IDIQ. The FAR also states that agencies may acquire commercial products or commercial services—which generally refer to qualifying products and services that are sold or made available to the general public—using streamlined procedures.¹² AI solutions may be commercial, and these procedures can help agencies acquire them faster.¹³

Established government-wide or agency-wide multiple-award contracts. Agencies can use the Federal Supply Schedule program, also known as the Multiple Award Schedule program, which is directed and managed by GSA and provides federal agencies with a simplified process for obtaining commercial supplies and services at prices associated with

¹¹The FAR and Defense FAR Supplement are currently undergoing a complete overhaul called the Revolutionary FAR Overhaul. The initiative began in April 2025 as directed by Executive Order 14275 (Restoring Common Sense to Federal Procurement) to restore the FAR to its statutory roots and remove most non-statutory rules or Executive Order, other than text essential to sound procurement. Exec. Order No. 14,275, 90 Fed. Reg. 16,447 (Apr. 15, 2025). The Revolutionary FAR Overhaul's rewrite of the FAR, called Phase 1, consisted of issuing model deviated text for the rewritten FAR parts. Starting in December 2025, DOD issued model deviation text for parts of the Defense FAR Supplement to align them with the Revolutionary FAR Overhaul. Phase 2 of the Revolutionary FAR Overhaul is ongoing, with the deviated FAR text going through rulemaking. This report's reference to the FAR and Defense FAR Supplement will be to the codified legacy FAR and Defense FAR Supplement as our substantive work was conducted prior to the FAR and Defense FAR Supplement deviations taking effect. However, since most federal agencies are no longer observing those provisions, we also describe the model deviation text, as appropriate.

¹²For the definition of a commercial product and commercial service, see FAR 2.101.

¹³Contracting officers can use streamlined solicitation procedures, which can reduce the time needed to solicit offers. See FAR subpart 12.6; FAR subpart 12.2 of the FAR model deviation text. For example, any acquisition that meets the definition of a commercial product or commercial service is generally exempt from the requirement to obtain certified cost or pricing data in order to determine price reasonableness. See FAR 15.403-1; FAR 15.403-2 of the FAR model deviation text.

volume buying.¹⁴ Schedules are catalogs of related products and services from preapproved vendors with established pricing that can be used by federal agencies to obtain goods and services, ranging from office furniture to medical equipment and supplies.¹⁵ When leveraging the Federal Supply Schedule, agencies can place orders using IDIQ contracts awarded by GSA.¹⁶

Agencies can also place orders using existing agency-wide vehicles such as blanket purchase agreements or multiple award IDIQ contracts. Blanket purchase agreements are agreements (not contracts) between government agencies and qualified vendors. They contain pre-negotiated terms and conditions, including prices, in place for future purchases and are a simplified method of fulfilling repetitive needs for supplies and services.¹⁷ IDIQ contracts can be used when the exact quantities and timing for products and services is not known at the time of award.¹⁸ Contracting officers are required, to the maximum extent practicable, to give preference to making multiple awards off IDIQ contracts under a single solicitation for the same or similar supplies or services to two or more sources.¹⁹ These contracts may be available for use within an agency or across multiple agencies.

Custom solutions. When existing contracts will not meet an agency's needs—for example, if commercial products or commercial services are not adequate to meet an agency's requirements—an agency may award a new contract. The exact type of contract awarded will vary depending

¹⁴For more information about GSA's Federal Supply Schedule program, see FAR subpart 8.4.

¹⁵Since 1960, GSA has delegated authority to VA to manage health care related schedules.

¹⁶For more information about procedures for placing orders or establishing blanket purchase agreements against a Federal Supply Schedule contract, see FAR 8.405 and subpart 538.71 deviation text. Blanket purchase agreements and orders placed against a Federal Supply Schedule contract using the procedures of that subpart are considered to be issued using full and open competition. See FAR 8.404(a) and 538.7102-1(a).

¹⁷See FAR 13.303 (FAR 12.201-1(e)(3) of the model deviation text). The FAR defines a blanket purchase agreement as a method of filling anticipated repetitive needs for supplies or services by establishing charge accounts with qualified sources of supply.

¹⁸See FAR 16.504-2.

¹⁹See FAR 16.504(c) and FAR 16.504-3(a)(1). Under a multiple award IDIQ contract, contracting officers generally must provide each awardee a fair opportunity to be considered for each order unless an exemption applies. See FAR 16.505(b)(1) and FAR 16.507.

on factors such as the degree to which the requirements have been defined. For example, a firm-fixed price contract may be used to acquire supplies or services when there are reasonably definite requirements allowing the contracting officer to establish fair and reasonable prices at the outset. If the requirements are less defined, preventing the negotiation of exact costs to be estimated with sufficient accuracy to use a fixed-price contract, a cost-reimbursement contract may be used, subject to certain limitations.²⁰

Intellectual property (IP). In addition to providing contracting mechanisms, the FAR also implements laws and provides the basic regulatory framework governing how agencies may license and acquire contractor IP.²¹ In general, using another entity's IP requires permission, and the government typically uses licenses to obtain permission and define the scope of its rights to use a particular contractor's IP. The federal government may also obtain data rights when the development of IP is funded by the government—in whole or in part—and the types of data rights obtained by the government can depend on how the IP is developed and funded.²²

Recent executive orders. In March and April 2025, the President issued executive orders that directed agencies to take steps to consolidate procurement in GSA and directed agencies to procure commercially available products and services to the maximum extent practicable.²³ Subsequently, OMB issued a memorandum stating that OMB and GSA would work closely with agencies to significantly increase consolidation efforts, noting that certain types of requirements are highly suitable for consolidation.²⁴ The Federal Acquisition Regulation Council also made changes to the FAR that generally require agencies to purchase

²⁰See FAR subpart 16.3.

²¹See FAR subpart 27.4. Agency supplements to the FAR may provide additional regulations governing licensing and acquisition of contractor intellectual property. See, for example, Defense FAR Supplement subpart 227.71.

²²Data rights are also determined by whether the item, process, or software is commercial or non-commercial, and the purpose of the data in question.

²³Exec. Order. No. 14,240, 90 Fed. Reg. 13,671 (Mar. 25, 2025); and Exec. Order. No. 14,271, 90 Fed. Reg. 16,433 (Apr. 15, 2025).

²⁴Office of Management and Budget, *Consolidating Federal Procurement Activities*, OMB Memorandum M-25-31 (Washington, D.C.: July 18, 2025). The memorandum notes that acquisitions with simple requirements that are easy to standardize, are mission agnostic, and require low levels of agency involvement are more suitable to consolidation.

commercial products and services when possible and to use the Federal Supply Schedules and government-wide contracts under certain circumstances.²⁵

In April 2025, the President issued an executive order directing OMB's Office of Federal Public Procurement Policy to coordinate with the Federal Acquisition Regulatory Council and appropriate agency leaders to overhaul the FAR.²⁶ These officials are directed to ensure that the FAR contains only provisions that are required by statute or that are otherwise necessary to support simplicity and usability, strengthen the efficacy of the procurement system, or protect economic or national security interests.²⁷ The FAR Council has issued guidance with new text by FAR part and agencies are generally expected to implement these changes by updating their own guidance. The FAR Council will later amend the FAR using formal rulemaking procedures.²⁸

Other transaction agreements. Congress also provided certain agencies with the authority to enter into other transaction agreements (OTA), which are generally not subject to the FAR. For example, DOD is able to enter into OTAs for research, prototyping, and follow-on production of new technologies or products, subject to certain conditions.²⁹ OTAs may be used to enable agencies to structure agreements that may leverage commercial business practices and

²⁵For example, the model deviation text for FAR 8.104(a)(1) states that agencies must use an existing contract or Blanket Purchase Agreement awarded for government-wide use, such as the Federal Supply Schedule, if the Office of Federal Procurement Policy has designated the contract as one that agencies must use unless an exception applies.

²⁶Exec. Order No. 14,275, 90 Fed. Reg. 15,621 (Apr. 9, 2025). This effort is also known as the Revolutionary FAR Overhaul.

²⁷The White House, *Restoring Common Sense to Federal Procurement*, (Washington, D.C.: Apr. 15, 2025). Exec. Order No. 14,275, 90 Fed. Reg. 16,447 (Apr. 15, 2025).

²⁸Office of Management and Budget, *Overhauling the Federal Acquisition Regulation*, OMB Memorandum M-25-26 (Washington, D.C.: May 2, 2025).

²⁹As of October 1, 2024, DHS's statutory authority to enter into other transactions has lapsed. In September 2025, DHS officials told us that the agency is actively pursuing legislative relief to restore this authority.

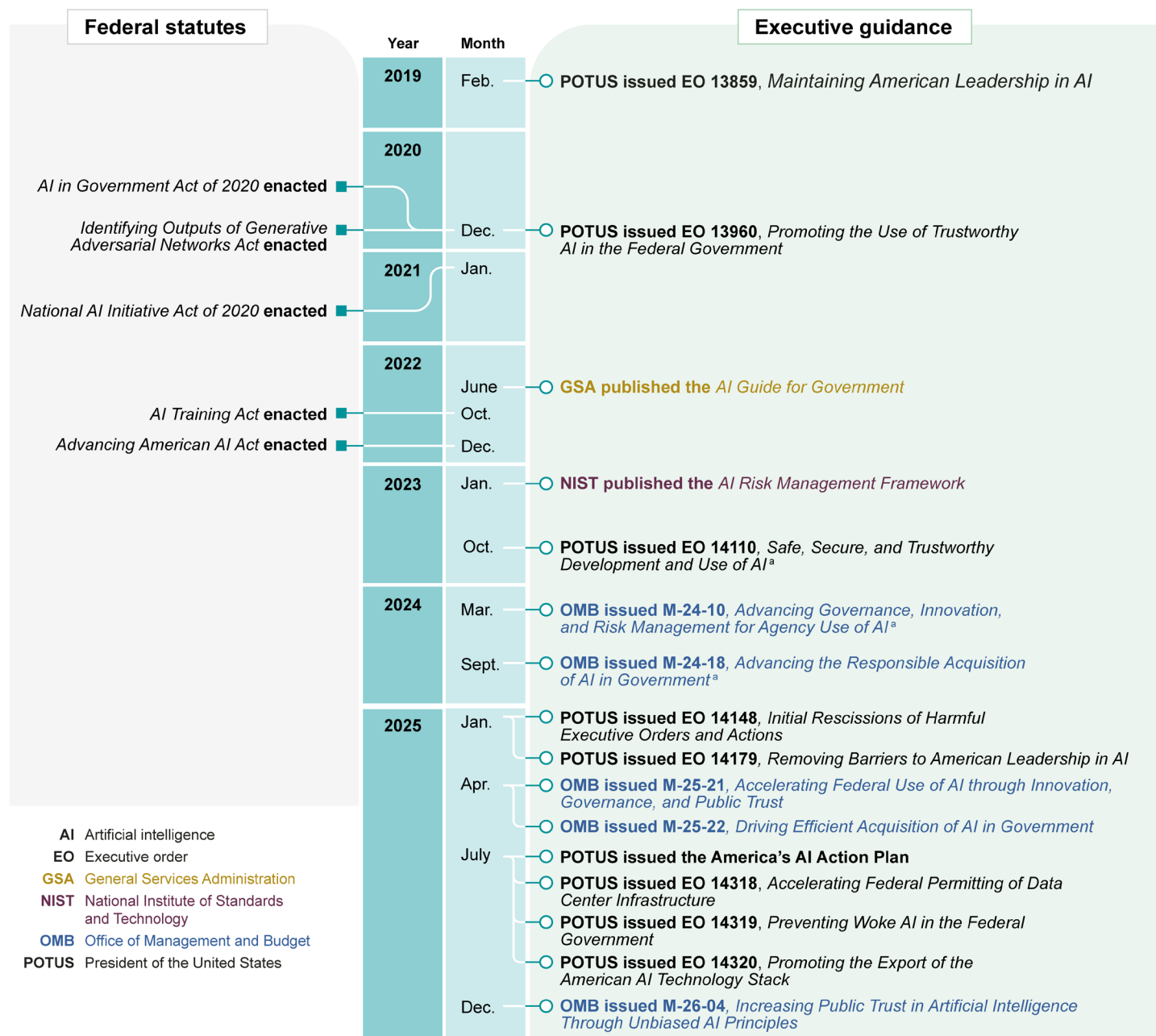
remove barriers to entry to encourage non-traditional contractors to do business with the government.³⁰

Federal Guidance on Agency Adoption of AI

Congress and the Executive Branch have taken several steps to improve federal AI adoption since 2019. Key legislative efforts have included requirements for certain agencies to develop AI use case inventories. Additionally, executive orders and OMB memorandums have provided guidance on federal government use of AI and ensuring responsible development and acquisition of AI capabilities, while GSA and NIST guidance provide federal agencies with information on building, investing in, and evaluating AI capabilities (see fig. 3).

³⁰OTAs do not always include default provisions that are ordinarily included in a FAR-based contract, such as clauses which may provide greater oversight into contractors' costs. Instead, contracting officials must determine what protections to include. For additional information, see GAO, *Other Transaction Agreements: Improved Contracting Data Would Help DOD Assess Effectiveness*, [GAO-25-107546](#) (Washington, D.C.: Sept. 3, 2025); *COVID-19 Contracting: Actions Needed to Enhance Transparency and Oversight of Selected Awards*, [GAO-21-501](#) (Washington, D.C.: July 26, 2021); *COVID-19: Critical Vaccine Distribution, Supply Chain, Program Integrity, and Other Challenges Require Focused Federal Attention*, [GAO-21-265](#) (Washington, D.C.: Jan. 28, 2021); and *Transportation Security Administration: After Oversight Lapses, Compliance with Policy Governing Special Authority Has Been Strengthened*, [GAO-18-172](#) (Washington, D.C.: Dec. 21, 2017).

Figure 3: Timeline of Key Artificial Intelligence Legislative and Executive Guidance



Source: GAO analysis of federal statutes, executive orders, and federal guidance related to AI and generative AI. | GAO-26-107859

^aEO 14148, issued in January 2025, rescinded EO 14110 and OMB memorandums M-24-10 and M-24-18.

In April 2025, OMB issued M-25-22, which provided government-wide guidance for AI acquisitions. OMB M-25-22 focuses on three overarching themes to help agencies responsibly acquire AI: ensure a competitive AI marketplace; track AI performance and manage risk; and promote cross-functional engagement. Within those areas, OMB identifies required or recommended actions for agencies across the acquisition life cycle (see table 1).

Table 1: Required or Recommended Agency Actions in OMB Guidance When Acquiring AI

Acquisition phase	OMB Guidance for Acquiring Artificial Intelligence (AI)
Pre-award	Agencies should: • Convene cross-functional teams to inform the procurement of AI systems in a streamlined manner • Conduct thorough market research when planning an acquisition • Include provisions in solicitations to encourage AI proposals that offer knowledge transfer, data and model portability, clear licensing terms, and pricing transparency, and • Consider using performance-based acquisition techniques, such as statements of objectives, performance work statements, quality assurance surveillance plans, and contract incentives
Award	Agencies should: • Include contract terms that address use of government data, intellectual property rights, privacy, and vendor lock-in, among other requirements Agencies are encouraged to: • Test proposed AI solutions to understand the capabilities and limitations before awarding contracts and throughout the acquisition lifecycle
Post-award	Agencies should: • Receive an authorization to operate AI systems and services from an appropriate official prior to deployment • Perform effective system oversight consistent with contract terms, and • Work with vendors to implement contractual terms related to rights and data after deciding not to extend contracts

Source: Office of Management and Budget (OMB) Memorandum M-25-22. | GAO-26-107859

Prior GAO Reports on AI

We previously reported on government-wide AI use case inventories and how federal agencies, including DOD and DHS, use AI for national security purposes.³¹ We also reported on specific types of AI, such as

³¹GAO, *Artificial Intelligence: Fully Implementing Key Practices Could Help DHS Ensure Responsible Use for Cybersecurity*, [GAO-24-106246](#) (Washington, D.C.: Feb. 7, 2024); *Artificial Intelligence: Agencies Have Begun Implementation but Need to Complete Key Requirements*, [GAO-24-105980](#) (Washington, D.C.: Dec. 12, 2023); *Facial Recognition Services: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties*, [GAO-23-105607](#) (Washington, D.C.: Sept. 5, 2023); and *Artificial Intelligence: DOD Needs Department-Wide Guidance to Inform Acquisitions*, [GAO-23-105850](#) (Washington, D.C.: June 29, 2023).

generative AI technologies, as well as related information technology developments, including cloud infrastructure and high-risk emerging technologies for cybersecurity.³² We also assessed how AI affects safety and the environment, and published an AI Accountability Framework to help federal managers ensure accountability and responsible use of AI.³³

As AI Technology Rapidly Evolves, Agencies Are Using a Wide Range of Acquisition Approaches

Agencies are increasingly adopting rapidly evolving AI capabilities to support their missions. For example, DOD is acquiring computer vision capabilities for military reconnaissance units, and VA is acquiring deep learning models to support veterans' health care. Agency officials told us AI solutions can offer previously unavailable capabilities or increase efficiency and speed in delivering services. To incorporate these capabilities into their operations, we found that agencies are experimenting with a wide range of AI acquisition approaches and pursuing strategic initiatives to improve AI acquisitions government-wide. However, in a landscape with rapidly evolving AI capabilities, markets, and federal policy, it is too soon to tell which approaches will most successfully meet agencies' requirements under different circumstances, and which initiatives will provide the best return on investment.

Agencies Are Increasingly Adopting Rapidly Evolving AI Capabilities to Support Their Missions

According to the Federal Chief Information Officer, federal agencies more than doubled their use of AI from 2023 to 2024, and congressional and executive branch efforts are underway to further adopt AI capabilities.³⁴ For example, Congress recently appropriated approximately \$1.7 billion for AI efforts across the government.³⁵ In addition, the White House

³²GAO, *Science & Tech Spotlight: AI Agents*, [GAO-25-108519](#) (Washington, D.C.: Sept. 10, 2025); *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, [GAO-25-107743](#) (Washington, D.C.: Feb. 25, 2025); and *Cloud Computing: Agencies Need to Address Key OMB Procurement Requirements*, [GAO-24-106137](#) (Washington, D.C.: Sept. 10, 2024); and [GAO-24-106946](#).

³³GAO, *Artificial Intelligence: Generative AI's Environmental and Human Effects*, [GAO-25-107172](#) (Washington, D.C.: Apr. 22, 2025); [GAO-24-106946](#); and [GAO-21-519SP](#).

³⁴Clare Martorana, "AI in Action: 5 Essential Findings from the 2024 Federal AI Use Case Inventory" (Jan. 15, 2025), <https://www.cio.gov/news/ai-in-action>.

³⁵An Act To provide for reconciliation pursuant to title II of H. Con. Res. 14, Pub. L. No. 119-21, 139 Stat. 72 (2025)(hereafter, the One Big Beautiful Bill Act).

released America’s AI Action Plan, which lays out plans to accelerate innovation and adoption of AI within federal agencies.³⁶

Officials at our five selected agencies told us AI solutions can offer new capabilities or more efficient delivery of services. For example, we found that DHS acquired machine learning and computer vision capabilities to quickly identify areas needing additional attention following natural disasters. We also found that VA acquired natural language processing capabilities to analyze veterans’ survey responses and benefits claims. In another example, GSA established partnerships with leading AI companies—OpenAI, Google, and Anthropic—to establish chatbot capabilities, among others, promising to increase the efficiency of administrative functions. Figure 4 provides illustrative examples of agencies’ use of AI to support their missions.

Figure 4: Selected Federal Government AI Solutions

 Artificial Intelligence (AI)		
	Machine Learning	Agencies we reviewed used machine learning for test and evaluation and cybersecurity anomaly detection.
	Deep Learning	Agencies we reviewed used deep learning to detect seizures and establish AI infrastructure.
	Generative AI	Agencies we reviewed used generative AI for chatbot capabilities and to develop hazard mitigation plans.
	Computer Vision	Agencies we reviewed used computer vision to support disaster recovery efforts and identify travelers using facial recognition.
	Natural Language Processing	An agency we reviewed used natural language processing to support benefits claims and suicide prevention efforts.

Source: GAO analysis of documentation from the General Services Administration and Departments of the Defense, Homeland Security, and Veterans Affairs; iierlok_xolms/stock.adobe.com (icons) and GAO (Computer Vision icon). | GAO-26-107859

³⁶The White House, *Winning the Race: America’s AI Action Plan* (Washington, D.C.: July 23, 2025).

Commercial developers are continually updating AI capabilities and fine-tuning models for specific uses, including uses at federal agencies, which have ranged from air traffic control to patent application reviews. Although the abundance of solutions and vendors provides federal agencies opportunities to improve their operations, in the past, rapid technological development rendered entire infrastructures or business cases obsolete. For example, a senior official at GSA compared the current AI environment to the abundance of search engines that emerged in the early 2000s. This official explained that agencies should avoid committing to the AI equivalents of AltaVista or Ask Jeeves, when competitors will likely ascend as Google did—becoming clear leaders in their respective fields.

Agencies Are Experimenting with Various Acquisition Approaches as They Adopt AI

Federal agencies generally have great latitude when determining which acquisition approach to use to meet a particular requirement, and that is true for AI acquisitions as well. This is because each acquisition is unique, and what works well under one set of circumstances may not work well under another. Through the end of fiscal year 2025, agencies were continuing to experiment with various acquisition approaches across a wide range of AI capabilities in an effort to effectively incorporate AI into their operations.

Agency-directed vs. vendor-driven. Some agencies seek solutions to meet key mission needs by awarding new contracts to develop or leverage specific AI capabilities. For example, DHS used GSA's Federal Supply Schedule to acquire generative AI capabilities that could help develop portions of hazard mitigation plans for local communities; in this case, those impacted by natural disasters. We also found that industry sometimes introduces capabilities, some of which are commercial, to agencies to meet their needs in the absence of specific AI requirements. For example, VA awarded a task order off a GSA schedule to acquire a medical software solution with AI capabilities. In another example, GSA acquired a facility and equipment maintenance tracking software that included a chatbot capability for customer service support. GSA officials told us that the vendor offered the chatbot as an added capability and not in response to a defined requirement.

The benefits of an agency-directed approach using typical acquisition planning steps include a deliberate decision-making process that involves AI terms and conditions that reflect agency requirements. However, this process can be lengthy and may slow the adoption of rapidly evolving AI capabilities. Alternatively, under a vendor-driven approach, particularly when commercial offerings are available, agencies can receive upgraded

capabilities more rapidly. However, not including AI terms and conditions when using this approach may increase the risk of experiencing unanticipated cost growth and operational challenges, such as “model drift”— decreasing reliability over time.

FAR-based contracts vs. other agreements. We reviewed several AI acquisitions that used different types of FAR-based contracts, including firm-fixed price contracts, to buy licenses for commercial AI solutions. For example, DHS used a firm-fixed price order to obtain a license for facial matching software for use across the department, including to assist with traveler identity verification at airports.

Alternatively, DOD leveraged its authority to use OTAs to develop AI capabilities. In July 2025, DOD awarded OTAs with \$200 million ceilings to four leading AI companies to accelerate adoption of advanced AI capabilities across the department.

In addition, the Air Force indicated it used another arrangement known as a partnership intermediary agreement to support the development of a chatbot similar to ChatGPT.³⁷ In this example, the Air Force partnered with the Wright Brothers Institute to expedite the transfer of technology, and procured expert assistance related to assessing technology capabilities and problem analyses by issuing an order under the agreement.

The potential benefits of using non-FAR-based contracts like OTAs and partnership intermediary agreements can include greater flexibility that may help address concerns from vendors who do not typically do business with the federal government. These concerns may include intellectual property rights, award time frames, and the need to establish government-unique cost accounting systems. However, we previously found that agencies’ use of OTAs carries the risk of reduced accountability and transparency compared to FAR-based contracts.³⁸ OMB M-25-22 states that agencies may need more transparency rather than less in contracts for AI systems that support “high-impact” use cases. For example, the memorandum states that agencies should

³⁷According to the Defense Acquisition University, a partnership intermediary agreement is a contract, agreement, or memorandum of understanding with a non-profit partnership intermediary to engage academia and industry on behalf of the government to accelerate tech transfer and licensing. See 15 U.S.C. § 3715 and 10 U.S.C. § 4124.

³⁸[GAO-21-501](#) and [GAO-21-265](#).

determine whether a system is likely to support “high-impact” AI use cases early in the acquisition life cycle, and inform vendors of the transparency and documentation requirements that must be met in solicitations for those systems.

Custom acquisitions vs. leveraging established contracts. Agencies acquired AI capabilities using direct contracts with vendors and agency or government-wide vehicles. For example, the VA awarded a new contract to a single vendor to develop AI capabilities for identifying suicidal ideation indicators in veterans’ survey responses after considering GSA schedule and other offerings in its market research.³⁹ According to OMB guidance, the custom approach is suitable when mission needs are specific and require a high level of agency involvement during contract performance.

Conversely, agencies can leverage existing agency or government-wide contracts, such as the GSA Federal Supply Schedule, to meet their needs. For example, GSA launched the OneGov Strategy in April 2025 to modernize how agencies can procure and manage information technology and other commodities from a broad range of vendors for government-wide use. According to GSA, the OneGov Strategy ensures transparent pricing, streamlines acquisitions, and improves cybersecurity protections while providing the entire federal government access to leading AI models. As part of this strategy, GSA reported entering into agreements with OpenAI, Anthropic, and Google for government-wide use in August 2025.⁴⁰ Similarly, we found DOD entered into agreements with multiple vendors when it established Tradewinds, an acquisition ecosystem meant to deliver emerging technologies across the department.

OMB guidance states that a key benefit of leveraging established contracts is increased efficiency. For example, under the GSA multiple award schedule, agencies can place orders against previously established blanket purchase agreements for which GSA has already negotiated prices for certain products and services. Such an approach can expedite the acquisition process for agencies by streamlining certain procedures. To this end, in July 2025, OMB directed agencies to

³⁹VA officials reported this program was retired in January 2023.

⁴⁰GSA officials told us that other vendors may be added under the OneGov Strategy in the future.

consolidate procurement through GSA, leveraging the agency's expertise in addressing prevalent and repetitive needs.⁴¹

AI as a service vs. as a product. When proactively acquiring AI, agency officials told us that they often acquire the AI capabilities as a service, rather than as a product, and most of the contracts and agreements we assessed as part of our in-depth reviews were for services. For example, the Air Force procured support for its development of generative AI capabilities as a service to provide chatbot support across the department. In addition, agency officials told us licensing agreements for software-as-a-service are frequently used for AI acquisitions. Most of the solutions we reviewed had contracts that included licenses, and most of those licenses were related to software procured as a service.⁴² For example, the Army's Project Linchpin included such license agreements in its contract that establish departmental AI infrastructure and a contract for test and evaluation services. This is consistent with guidance in OMB M-25-22, which recognizes acquired AI as systems or services. OMB guidance also encourages agencies to use Quality Assurance Surveillance Plans to assess both product and service contracts.

Agencies in our sample sometimes purchased software as a product, but AI systems—as defined in federal statute—continuously learn from experience by improving performance when exposed to new data.⁴³ As such, AI solutions require ongoing assessment to ensure models produce accurate results, which is conceptually different than acquiring products.

Additionally, agency officials who manage some of the most sophisticated AI solutions in our sample asserted that the quality of services vendors provide affects performance outcomes more than the quality of model

⁴¹Office of Management and Budget, *Consolidating Federal Procurement Activities*, OMB Memorandum M-25-31 (Washington, D.C.: July 18, 2025).

⁴²According to NIST guidance, software-as-a-service delivers one or more applications and all the resources (operating system and programming tools) and underlying infrastructure, which an agency can use on demand. This differs from service models such as infrastructure as a service, which delivers and manages the basic computing infrastructure of servers, software, storage, and network equipment and platform as a service, which delivers and manages the infrastructure, operating system, and programming tools and services that an agency can use to create applications. See National Institute of Standards and Technology, Special Publication 800-145.

⁴³James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. Law 117-263, title 72 (2022) (codified at 40 U.S.C. § 11301 note). John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. Law 115-232, Section 238g. (10 U.S.C. 2358 note).

algorithms (i.e., the core software product). For these reasons, we found that acquiring AI as a service can often be a preferred approach.

Some Agencies Are Pursuing Strategic Initiatives Intended to Improve AI Acquisitions Government-Wide

GSA and NIST—a bureau of the Department of Commerce—are pursuing strategic initiatives focused on improving AI acquisitions government-wide. These initiatives involve efforts to train the workforce on AI and improve evaluations of AI vulnerabilities and threats.

GSA has established a government-wide AI community of practice intended to encourage collaboration among federal agencies, enhance workforce capacities, and support the integration of AI to meet mission needs. GSA holds monthly meetings to inform agency personnel on topics such as federal guidance for acquiring and incorporating AI systems and commercial AI offerings for federal government use.

NIST has established the Center for AI Standards and Innovation to facilitate testing and collaborative research intended to harness and secure the potential of commercial AI systems.⁴⁴ As part of its efforts to support safe development of AI systems, the center intends to collaborate with various federal agencies and the private sector to conduct security evaluations and assessments of AI systems, as well as develop methods others can use to evaluate such systems.

Agencies Face Strategic and Programmatic Challenges When Acquiring AI Capabilities

Agencies reported facing strategic and programmatic challenges across the acquisition life cycle. Officials told us the strategic challenges broadly affected their ability to acquire AI solutions across their agencies. They told us the programmatic challenges more narrowly affected the ability of individual programs to procure desired capabilities. Table 2 summarizes challenge areas identified by agency officials.

Table 2: Key Procurement Challenge Areas Identified by Selected Agencies	
Strategic	Programmatic
Access to subject matter experts	Requirements definition and contract terms
Protections for government data and intellectual property rights	Early testing and continuous evaluation
Traditional acquisition time frames and contract approaches	Artificial intelligence pricing and overall cost

Source: GAO analysis of interviews with officials from the General Services Administration and Departments of Commerce, Defense, Homeland Security, and Veterans Affairs. | GAO-26-107859

⁴⁴The Center for AI Standards and Innovation was previously known as the U.S. AI Safety Institute.

In April 2025, OMB issued guidance to help agencies acquire AI responsibly. OMB directed agencies to update their AI policies to comply with that high-level guidance, which we found corresponds to key acquisition challenges that agency officials identified.

Access to subject matter experts. Officials from each of our five selected agencies told us that limited access to subject matter experts, such as data scientists and software engineers, was a challenge for procuring AI technologies. Some of these officials asserted that subject matter experts are critical for defining requirements, such as data and infrastructure needs, and evaluating vendor proposals. For example, officials with VA's Automated Decision Support effort told us they struggled to establish effective evaluation factors for source selection due to limited technical expertise. They clarified that having the right technical experts involved at the award phase of the acquisition life cycle is necessary to select vendors with the greatest ability to accelerate benefits delivery to veterans and their families.

Officials supporting other AI efforts told us technical experts can help understand AI risks, establish performance metrics, and evaluate post-award performance. For example, at DHS, officials supporting the Cybersecurity and Infrastructure Security Agency's Network Anomaly Alerting acquisition stated that they rely on subject matter experts to provide post-award vendor oversight to ensure efficient cyber threat detection. Officials told us that they faced challenges in having access to data scientists and cybersecurity experts. As a result, they reported encountering delays in completing acquisition tasks.

The strategic challenge of limited access to subject matter experts is reflected in OMB's April 2025 guidance on AI acquisitions. Specifically, OMB M-25-22 directs agencies to convene cross-functional teams of agency officials with relevant expertise, including those with expertise in acquisition, IT, cybersecurity, privacy, confidentiality, civil rights, civil liberties, budgeting, data, legal, program evaluation, and other areas as necessary.⁴⁵

⁴⁵OMB M-25-22 also states that cross-functional teams should inform the procurement of AI systems or services in a streamlined manner that apportions time and resources according to the requirements of the procurement, including associated complexity and risk, to support effective, efficient, and responsible development and execution of ongoing performance monitoring.

Protections for government data and IP rights. Officials from each of our five selected agencies identified establishing data ownership and IP rights as a challenge to acquiring AI. Some officials leading more established acquisitions stressed that data is paramount for effective AI outcomes, and they asserted that the government should prioritize data ownership over acquiring algorithms. In the past, we found that DOD reported facing challenges related to reduced mission readiness and increased sustainment costs when it did not acquire, or was unable to acquire, necessary data rights for weapons systems.⁴⁶

Officials from the Federal Emergency Management Agency's (FEMA) Geospatial Damage Assessment solution told us they could not share model outputs with other federal and state partners because they did not obtain certain data rights at the award phase. Officials added that the ability to share such data with their partners post-award would be key for supporting disaster recovery as AI takes a larger role in future acquisitions.

Additionally, officials from the National Geospatial-Intelligence Agency (NGA) Maven program reported challenges determining the appropriate level of IP and data rights needed in the pre-award phase to promote future competition. They indicated a 2-day data rights summit with legal, program, and contracting personnel was held to discuss IP and data rights issues and appropriate contract language. However, following this summit, those officials expressed a continuing need for additional training on IP rights clauses for AI contracts.

OMB M-25-22 generally requires agencies to include contract terms that address IP rights and protect government data. Specifically, the memorandum directs agencies to have appropriate processes that address the use of government data and include appropriate contract terms that delineate the government and contractor's respective ownership and IP rights. OMB M-25-22 also directs each agency to revisit, and update where necessary, its process for determining data ownership and IP rights in procurements for AI solutions and prioritize standardization across contracts where possible. This direction

⁴⁶GAO, *Weapon System Sustainment: DOD Can Improve Planning and Management of Data Rights*, [GAO-25-107468](#) (Washington, D.C.: Sept. 29, 2025); and *Defense Acquisitions: DOD Should Take Additional Actions to Improve How it Approaches Intellectual Property*, [GAO-22-104752](#) (Washington, D.C.: Nov. 30, 2021).

corresponds to the strategic challenge of protecting government data and IP rights that we found at the agencies we reviewed.

Traditional acquisition time frames and contract approaches. In the past, we found that the use of IDIQ and government-wide contracts can reduce administrative burden and increase efficiencies.⁴⁷ Officials from each of our five selected agencies identified traditional acquisition time frames and approaches as poorly aligned with the speed of AI development.

Officials from the Army's Project Linchpin explained that the traditional approach of developing a system for 5 years, followed by operations and maintenance, does not reflect the realities of AI. Similarly, senior leaders from VA told us that FAR-based contracts can take 2 years to award, explaining that many agencies struggle to move from pilot to production more quickly because of market research requirements and a contract approval process that can take up to a year. They added that, at this pace, agencies are no longer purchasing innovation.

Additionally, officials from FEMA's Planning Assistance for Resilient Communities acquisition told us they could not meet key deadlines by following the traditional acquisition process to award a new contract for their specific requirements. They determined that using an existing contract was more expedient but limited the specific AI terms and conditions they could include. As a result, they told us they could not require the vendor to perform post-award testing to improve hazard mitigation planning features under the existing contract terms.

OMB M-25-22 directs GSA to develop a plan to release guides that address potential acquisition authorities, approaches, and vehicles for AI procurement, corresponding to the strategic challenge posed by traditional acquisition time frames and contract approaches at the agencies we reviewed. The memorandum also strongly encourages agencies to use performance-based acquisition techniques, such as using statements of objectives or performance work statements instead of traditional statements of work that may introduce limitations.

⁴⁷GAO, *Federal Buying Power: OMB Can Further Advance Category Management Initiative by Focusing on Requirements, Data, and Training*, [GAO-21-40](#) (Washington, D.C.: Nov. 30, 2020); and *Federal Contracts: Agencies Widely Used Indefinite Contracts to Provide Flexibility to Meet Mission Needs*, [GAO-17-329](#) (Washington, D.C.: Apr. 13, 2017).

Requirements definition and contract terms. Officials from all five of our selected agencies identified defining requirements and contract terms as challenges. Some officials explained that well-defined requirements are needed to develop contract terms and performance metrics that allow agencies to meet mission needs, evaluate AI performance, and hold vendors accountable. For example, NGA officials told us that DOD initially funded Maven without well-defined or documented requirements to prioritize acquiring new capabilities as quickly as possible. These officials learned that without clear requirements defined in contracts they could not hold vendors accountable for weekly deliverables needed for Agile development. As a result, they are now adding metrics and model performance requirements before awarding follow-on contracts to better evaluate what vendors deliver against user needs. GAO has previously reported on challenges agencies have faced related to requirements definition and contract terms.⁴⁸

In another example, officials with VA's Automated Decision Support effort told us that VA's standard contract language for AI is outdated. Specifically, officials reported that VA's standard security language was not sufficient for the program's requirements for protecting veterans' information in a rapidly changing environment. As a result, officials reported working to develop more comprehensive security terms to meet mission needs. Officials added that it would be helpful to have government-wide, standard contract language to help hold vendors accountable for information security risk.

The programmatic challenge of defining requirements and contract terms is reflected in OMB M-25-22. The memorandum states that the government must communicate clear and specific requirements that make it easy for vendors to offer state-of-the-art AI capabilities to support efficient and effective public services. It strongly encourages agencies to focus on desired performance outcomes to identify requirements and directs agencies to include appropriate contract terms related to privacy, competition, testing requirements, and risk management practices.

Early testing and continuous evaluation. Officials from all five of our selected agencies identified challenges with determining the appropriate methods to test and evaluate AI technologies before and after award phases, citing the diversity and complexity of the systems, and need for

⁴⁸GAO, *Federal Acquisitions: Congress and the Executive Branch Have Taken Steps to Address Key Issues, but Challenges Endure*, [GAO-18-627](#) (Washington, D.C. Sept. 12, 2018).

robust, continuous testing. For example, NIST officials stated that well-defined, universal AI tests do not exist yet because of the variation and complexity of AI services.

Officials from multiple agencies also highlighted the need for continuous testing to prevent suboptimal or deteriorating AI model performance. For example, GSA officials supporting the USAi effort—a platform that provides agencies access to several generative AI models for chat-based AI and administrative support—told us that to address challenges with evaluating model performance, they are testing leading AI models against a battery of performance tests to evaluate results over time. They added that such testing is critical to be able to determine if new versions of those models justify their often much higher prices. Further, GSA officials told us that “high-impact” use cases also require additional testing and ongoing performance monitoring throughout the acquisition life cycle, which is consistent with OMB guidance.

OMB M-25-22 states that agencies should test proposed AI solutions to understand their capabilities and limitations before awarding contracts and should be able to regularly monitor and evaluate an AI system throughout its acquisition life cycle.⁴⁹ OMB M-25-22 also states that agencies should use data they have defined for validation and testing when conducting any independent evaluations. Specifically, the data should not be accessible to the vendor and should be as similar as possible to the data used when the system is deployed. That direction corresponds to the programmatic challenge of early testing and continuous evaluation that we found at the agencies we reviewed.

AI pricing and overall cost. Officials from all five of our selected agencies told us it is challenging to understand AI costs, particularly in rapidly evolving markets. These officials also cited uncertainty related to how vendors price AI-related licenses and services. For example, officials from the Army’s XM-30 AI solution, which provides enhanced targeting for its minimally crewed infantry combat vehicles, stated that AI licensing fees can be exorbitant, citing proposals that included prices for around \$300,000 per vehicle per year. That proposal would have resulted in more than \$500 million each year just for licensing fees in addition to the cost to acquire the vehicles. Army officials reported that they rejected this

⁴⁹NIST’s AI Risk Management Framework also states that test and evaluation can provide insights relative to technical standard and norms and allow for pre-deployment remediation and risk management. National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework*, NIST AI 100-1 (January 2023).

proposal, and they are exploring more affordable licensing models for their fleet.

Additionally, officials supporting the Army's Project Linchpin explained that government buyers often underestimate overall costs because they only consider the cost to train AI models and overlook the infrastructure needed to support AI capabilities over time. These officials explained that programs find it difficult to understand how enterprise-level costs, like cloud infrastructure or computing power, will change in the future because they are more familiar with traditional hardware acquisitions. As a result, agencies may find that AI solutions they acquire may be too expensive to sustain over time.

OMB M-25-22 states that agencies must procure effective and trustworthy AI capabilities in a timely and cost-effective manner, and should include pricing transparency provisions in solicitations, to the extent consistent with other law and policy. The memorandum also states that agencies should perform evaluations to determine the value of the solution to the government throughout the acquisition life cycle. Such evaluations should consider comparative system effectiveness and any ongoing operation and maintenance costs. This direction corresponds to the programmatic challenge of AI pricing and overall cost that we found at the agencies we reviewed.

Knowledge Sharing Can Help Agencies Apply Lessons Learned

OMB M-25-22 states that agencies should share knowledge and resources about AI acquisitions—including tools and best practices, such as language for standard contract clauses—through a web-based repository developed by GSA. However, we found that agencies we reviewed are not consistently prepared to address knowledge sharing. Specifically, the agencies in our scope are not systematically collecting lessons learned from AI acquisitions, including when an acquisition was discontinued.

For example, VA officials told us they decided to retire the SoKAT solution, which supported suicide prevention efforts, in January 2023, after officials determined that it did not improve upon existing solutions enough to justify the additional cost. VA officials supporting that solution told us they did not document lessons learned, which was a missed opportunity because VA has several other AI acquisitions related to suicide prevention among veterans. These acquisitions could have benefitted from lessons learned by the SoKAT solution and helped increase the likelihood that their solutions justified the additional cost.

Similarly, FEMA officials told us they did not document input that they shared with the Geospatial imaging vendor to improve model accuracy for identifying damage caused by natural disasters. Specifically, they did not document that they found the AI model struggled to distinguish between different types of dwellings. Those officials also anticipated accuracy issues would arise when the model assessed imagery from different regions than the imagery used to train it. We found that FEMA recently opted to continue using that vendor for disaster relief purposes for another 12-month period. In the future, other FEMA personnel using the same contract to meet their disaster recovery needs across the country may not benefit from early knowledge gained on how reliably the vendor's AI system performed.

Table 3 identifies two illustrative examples of AI acquisitions that took steps to address key challenges and identified lessons learned that could also benefit other AI acquisitions.

Table 3: Lessons Learned Related to Key Artificial Intelligence (AI) Acquisition Challenges

Key challenges identified by agency officials	Lessons Learned	
	DOD's Maven Acquisition	GSA's USAi Acquisition
Access to subject matter experts	To inform key decisions across the acquisition life cycle, Maven officials reported developing a web of cross-functional teams that include computer scientists, software engineers, test and evaluation officials, cybersecurity experts, and product managers.	To support the USAi acquisition, GSA officials reported that GSA's Chief AI Information, Privacy, and Cybersecurity Officers closely coordinated to ensure access to relevant subject matter experts.
Protections for government data and intellectual property rights	As they executed subsequent contract actions, Maven officials reported developing more specific terms and conditions addressing data ownership and data rights.	GSA developed a USAi privacy policy and contract language that clearly outline data ownership expectations and limits how vendors can access chat interaction data.
Traditional acquisition time frames and contract approaches	Maven officials reported using Agile software acquisition approaches, such as weekly planning meetings and 90-day sprints to deliver capabilities to end-users at a relatively rapid pace.	GSA officials announced partnerships with leading generative AI vendors—including Anthropic, OpenAI, and Google—to create a solution that allows federal agencies to quickly acquire chatbot capabilities through USAi and leverage the cloud infrastructure needed to access the vendors' models.
Requirements definition and contract terms	Maven officials reported learning that their early contracts lacked AI-related requirements needed to hold vendors accountable, and they added increasingly defined AI-related requirements in follow-on contracts.	GSA officials reported reusing contract terms for USAi that were effective in previous AI acquisitions, for example contractual frameworks defining service expectations.
Early testing and continuous evaluation	Maven officials reported awarding relatively small contracts to several AI vendors to test their solutions prior to committing to larger acquisitions.	GSA officials reported they are testing multiple AI capabilities through a suite of reliability tests before awarding multi-year USAi contracts.

Lessons Learned

**Key challenges
identified by
agency officials**

DOD's Maven Acquisition

GSA's USAi Acquisition

AI pricing and overall cost

Maven officials reported studying AI acquisition costs over time to inform a comprehensive cost-estimate that accounts for critical capabilities and sustainment costs.

GSA officials reported pursuing a usage pricing model for USAi rather than a licensing approach to reduce overall costs, explaining that most employees are not expected to use the capability extensively. In addition, GSA reported using structured pricing to account for complexity of expected model usage so that agencies do not pay more than needed for simple prompts or more sophisticated model features.

Source: GAO analysis of Department of Defense (DOD) and General Services Administration (GSA) documentation and interviews with agency officials. | GAO-26-107859

Agency officials from DOD, DHS, GSA, and VA told us they did not systematically document lessons from their AI acquisition efforts because their departmental policies and guidance do not require them to do so. Our review of the four agencies' departmental AI policies confirmed that none of the policies include a formal requirement or process to consistently document lessons learned even though some articulate their value.⁵⁰ Senior leaders confirmed that the departmental policies in effect as of September 2025 do not require agency officials to systematically document lessons learned from AI acquisitions.

Government-wide guidance from OMB M-25-22 is expected to be implemented at the agency level through departmental policies, per the memorandum. OMB directed agencies to update their AI policies to comply with the requirements in M-25-22 by December 29, 2025. In the past, we reported that agency-level implementation is critical to achieving the advantages of government-wide acquisition improvement efforts directed by OMB.⁵¹ For example, we found that VA had not fully

⁵⁰DOD's Responsible AI Strategy and Implementation Pathway highlights the importance of knowledge sharing and tasks the Chief Digital and Artificial Intelligence Office, in coordination with the Office of the Under Secretaries for Acquisition and Sustainment and Research and Engineering, with developing an Acquisition Toolkit to include—among other things—standard language for solicitations, AI system evaluation criteria, and contract clauses for test and evaluation, performance monitoring, and appropriate data deliverables and rights. As of September 2025, DOD's Acquisition Toolkit is reportedly under development. Department of Defense, *Responsible Artificial Intelligence Strategy and Implementation Pathway* (June 2022).

GSA's AI Guide for Government highlights the importance of using lessons learned to improve outcomes and help less-experienced personnel. General Services Administration, *AI Guide for Government*, June 2022.

⁵¹GAO, *VA Acquisitions: Leadership Accountability and Savings Goals Needed to Improve Purchasing Efficiency*, [GAO-25-107398](#) (Washington, D.C. Sept. 2, 2025).

implemented its category management policy in response to OMB guidance, missing opportunities to save billions of dollars.

Without systematic, robust knowledge sharing, federal buyers are more likely to make avoidable mistakes across the acquisition life cycle when they buy AI in the future. Officials from all of our selected agencies told us they had to figure out how to acquire AI on their own, and that having lessons learned from other federal AI buyers to apply would help them achieve better AI acquisition outcomes. They also told us that having agency-vetted terms and conditions to include in contracts would be beneficial.

Conclusions

Federal agencies are navigating a rapidly evolving AI landscape where capabilities, markets, and government-wide acquisition guidance are in flux. These agencies have wide latitude to acquire AI solutions in multiple ways, including as products and services, with new and existing contract vehicles, and through a variety of acquisition approaches. Agency officials face many procurement challenges as they try to determine which acquisition approaches best suit their needs. OMB's April 2025 guidance is a good starting point to address these challenges, but agencies need to follow through with their own policies. Among other things, this OMB guidance states that agencies should share knowledge and resources through a GSA-developed repository. However, we found DOD, DHS, GSA, and VA were not prepared to meet this provision. This lack of preparation stems from an absence of processes or requirements in agency policies to systematically collect lessons learned from AI acquisitions. Until agencies take action, they are missing opportunities to learn from more established acquisitions and increasing the risk that their future AI procurement efforts will repeat avoidable, and potentially costly, mistakes.

Recommendations for Executive Action

We are making a total of four recommendations: one to DOD, one to DHS, one to GSA, and one to VA. Specifically:

The Secretary of Defense should ensure that the Under Secretary of Defense for Acquisition and Sustainment updates the department's policies to establish processes and require officials to systematically collect lessons learned from AI acquisitions—including best practices involving contract clauses—and submit them to the GSA-managed repository to enable sharing and application by other agencies. (Recommendation 1)

The Secretary of Homeland Security should ensure that the Under Secretary for Management updates the department's policies to establish processes and require officials to systematically collect lessons learned from AI acquisitions—including best practices involving contract clauses—and submit them to the GSA-managed repository to enable sharing and application by other agencies. (Recommendation 2)

The Administrator of the General Services Administration should ensure that the Chief Acquisition Officer updates the agency's policies to establish processes and require officials to systematically collect lessons learned from AI acquisitions—including best practices involving contract clauses—and submit them to the GSA-managed repository to enable sharing and application by other agencies. (Recommendation 3)

The Secretary of Veterans Affairs should ensure that the Principal Executive Director of the Office of Acquisition, Logistics, and Construction updates the department's policies to establish processes and require officials to systematically collect lessons learned from AI acquisitions—including best practices involving contract clauses—and submit them to the GSA-managed repository to enable sharing and application by other agencies. (Recommendation 4)

Agency Comments

We provided a draft of this report to Commerce, DOD, DHS, GSA, and VA for review and comment. DOD, DHS, GSA, and VA concurred with our four recommendations and identified plans to address them in responses reproduced in appendices II – V. For example, DHS plans to update its departmental guidance, including its current AI procurement process guide, to ensure it contains systematic collection and documentation of lessons learned from AI acquisitions by July 2026. Commerce and DHS also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees and the Secretaries of the Departments of Commerce, Defense, Homeland Security, and Veterans Affairs; and the Administrator of the General Services Administration. In addition, the report is available at no charge on the GAO website at <https://www.gao.gov>.

If you or your staff have any questions about this report, please contact William Russell at RussellW@gao.gov and Candice N. Wright at WrightC@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this

report. GAO staff who made key contributions to this report are listed in appendix VI.

//SIGNED//

William Russell
Director, Contracting and National Security Acquisitions

//SIGNED//

Candice N. Wright
Director, Science, Technology Assessment, and Analytics

Appendix I: Sample of 13 AI Acquisitions from Selected Agencies

Table 4: GAO Sample of 13 AI Acquisitions from Selected Agencies

Agency	Selected AI Acquisitions
DHS	Advanced Network Anomaly Alerting. DHS’s Cybersecurity and Infrastructure Security Agency uses machine learning to provide analytic cybersecurity support and anomaly detection.
	Geospatial Damage Assessments. DHS’s Federal Emergency Management Agency (FEMA) uses machine learning and computer vision to analyze structural damage caused by natural disasters based on aerial imagery. In February 2026, DHS officials reported this effort has been retired and is no longer in use at FEMA.
	Planning Assistance for Resilient Communities. DHS’s FEMA uses generative AI to help develop hazard mitigation plans. In February 2026, DHS officials reported this effort has been retired and is no longer in use at FEMA.
	TSA PreCheck Touchless Identity Solution. DHS’s Transportation Security Administration (TSA) uses neural networks and computer vision to provide facial comparison for airport security.
DOD	NIPRGPT. The Air Force uses generative AI to provide chatbot support across the department.
	Cyclops. The Army uses computer vision to enhance targeting for the XM-30 class of combat vehicles.
	Project Linchpin. The Army uses AI capabilities such as machine learning, computer vision, and deep learning, as part of its effort to establish departmental AI infrastructure and deliver test and evaluation services.
	Maven. DOD’s National Geospatial-Intelligence Agency uses machine learning and computer vision to analyze geospatial imagery to identify potential targets for people to assess.
GSA	National Computerized Maintenance Management System Chatbot. GSA uses generative AI to provide facilities-specific support across the department.
	USAi. GSA uses generative AI to provide chatbot capabilities across the federal government.
VA	Automated Decision Support. VA’s Veterans Benefits Administration uses machine learning, computer vision, and natural language processing to assess veterans claims benefits.
	Persyst Analysis Software. VA’s Veterans Health Administration uses deep learning to provide trend analysis and seizure detection support for veterans.
	SoKat Suicidal Ideation Engine. VA’s Veterans Health Administration used natural language processing to review veterans’ survey responses for signs of suicidal ideation to alert crisis responders. VA retired this system in January 2023 without entering production.

Source: GAO analysis of documentation from the General Services Administration (GSA) and Departments of Homeland Security (DHS), Defense (DOD), and Veterans Affairs (VA). | GAO-26-107859

Appendix II: Comments from the Department of Defense



OFFICE OF THE ASSISTANT SECRETARY OF WAR
3600 DEFENSE PENTAGON
WASHINGTON, DC 20301-3600

Mr. William Russell
Director, Contracting and National Security Acquisitions
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Mr. Russell,

This letter serves as the Department of War response to the Government Accountability Office (GAO) Draft Report GAO-26-107859, titled, "ARTIFICIAL INTELLIGENCE ACQUISITIONS: Agencies Should Collect and Apply Lessons Learned to Improve Future Procurements".

Attached is the Department's draft response to the subject report. For further information, please contact Office of the Under Secretary of War for Acquisition and Sustainment, Mr. Sean Curl, Joint Analysis & Acquisition (JAA) Deputy Director, who may be reached at sean.e.curl.civ@mail.mil or 703-697-9275.

Sincerely,

CADMAN.DAVID
S.1229303615
Digitally signed by
CADMAN.DAVID.S.1229303615
Date: 2026.03.13 15:50:44 -0400 For

James A. Ruocco
Performing the Duties of Assistant Secretary
of War for Acquisition

**GAO DRAFT REPORT DATED JANUARY 15, 2026
GAO-26-107859 (GAO CODE 107859)**

**“ARTIFICIAL INTELLIGENCE ACQUISITIONS: AGENCIES SHOULD COLLECT
AND APPLY LESSONS LEARNED TO IMPROVE FUTURE PROCUREMENTS”**

**DEPARTMENT OF WAR COMMENTS
TO THE GAO RECOMMENDATIONS**

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense should ensure that the Under Secretary of Defense for Acquisition and Sustainment updates the department’s policies to establish processes and require officials to systematically collect lessons learned from AI acquisitions-including best practices involving contract clauses-and submit them to the GSA-managed repository to enable sharing and application by other agencies.

DOW RESPONSE: The Department of War concurs with this recommendation.

Appendix III: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

BY ELECTRONIC SUBMISSION

February 13, 2026

William Russell
Director, Contracting and National Security Acquisitions
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Candice N. Wright
Director, Science, Technology Assessment, and Analytics
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to GAO-26-107859, "ARTIFICIAL INTELLIGENCE ACQUISITIONS: Agencies Should Collect and Apply Lessons Learned to Improve Future Procurements"

Dear, Mr. Russell and Ms. Wright:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS, or the Department) appreciates the U.S. Government Accountability Office's (hereafter referred to as "the auditors") work in planning and conducting its review and issuing this report.

DHS leadership is pleased to note the auditors' recognition that DHS use of artificial intelligence solutions offers new capabilities and more efficient delivery of services, such as machine learning and computer vision capabilities to quickly identify areas needing additional attention following natural disasters. DHS remains committed to strengthening policies and processes for systematic collection of lessons learned from artificial intelligence acquisitions, such as by adding best practices involving contract terms and conditions into a General Services Administration-managed repository to promote sharing across agencies.

**Appendix III: Comments from the Department
of Homeland Security**

The draft report contained four recommendations, including one for DHS with which the Department concurs. Enclosed find our detailed response to the recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for the auditors' consideration, as appropriate.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JEFFREY M. BOBICH

Digitally signed by
JEFFREY M. BOBICH
Date: 2026.02.13
14:12:41 -0500

JEFFREY M. BOBICH
Director of Financial Management

Enclosure

**Enclosure: Management Response to Recommendations
Contained in GAO-26-107859**

The auditors recommended that the Secretary of Homeland Security ensure that the Under Secretary for Management:

Recommendation 2: Updates the department's policies to establish processes and require officials to systematically collect lessons learned from AI [artificial intelligence] acquisitions—including best practices involving contract clauses—and submit them to the [General Services Administration]-managed repository to enable sharing and application by other agencies.

Response: Concur. DHS, led by the Office of the Chief Information Officer, will update our current artificial intelligence procurement process guide to ensure it contains a section on the systematic collection and documentation of lessons learned from artificial intelligence acquisitions. Once updated, DHS personnel will use this process guide to share best practices and key insights both within the Department and with other federal agencies, as appropriate. This process guide will also align with Office of Management and Budget Memorandum M-25-22,¹ which provides guidance to federal agencies to acquire artificial intelligence systems in a way that is efficient, competitive, and cost-effective while managing risks, and protecting privacy and government data. In addition, the Office of the Chief Information Officer will lead DHS efforts to revise any existing policies and procedures as needed to institutionalize this approach and to promote continuous improvement in artificial intelligence procurement. Estimated Completion Date: July 31, 2026.

¹ M-25-22, "Driving Efficient Acquisition of Artificial Intelligence in Government," dated April 3, 2025.

Appendix IV: Comments from the General Services Administration

DocuSign Envelope ID: 7517D5CB-AB4D-455E-90A0-982A14ABD84E



**U.S. General Services
Administration**

February 12, 2026

The Honorable Orice Williams Brown
Acting Comptroller General of the United States
U.S. Government Accountability Office
Washington, DC 20548

Dear Acting Comptroller General:

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the U.S. Government Accountability Office (GAO) draft report, *Artificial Intelligence Acquisitions: Agencies Should Collect and Apply Lessons Learned to Improve Future Procurements* (GAO-26-107859).

GAO made the following recommendation to GSA:

The Administrator of the General Services Administration should ensure that the Chief Acquisition Officer updates the agency's policies to establish processes and require officials to systematically collect lessons learned from AI acquisitions—including best practices involving contract clauses—and submit them to the GSA-managed repository to enable sharing and application by other agencies. (Recommendation 3)

GSA agrees with the recommendation and has a plan to address it.

If you have any questions or require additional information, please contact the GSA Office of Congressional and Intergovernmental Affairs, at GSACongressionalAffairs@gsa.gov.

Sincerely,

A handwritten signature in blue ink, appearing to read "E. Frost".

Edward C. Frost
Administrator

U.S. General Services Administration
1800 F Street NW
Washington DC 20405-0002
www.gsa.gov

Appendix V: Comments from the Department of Veterans Affairs



DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON

March 3, 2026

Mr. William Russell
Director
Contracting and National Security Acquisitions
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Russell:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report: ***Artificial Intelligence Acquisitions: Agencies Should Collect and Apply Lessons Learned to Improve Future Procurements*** (GAO-26-107859).

The enclosure contains the action plan to address the draft report recommendation. VA appreciates the opportunity to comment on your draft report.

Sincerely,

A handwritten signature in black ink, appearing to read "Curt Cashour".

Curt Cashour
Chief of Staff

Enclosure

Appendix V: Comments from the Department
of Veterans Affairs



DEPARTMENT OF VETERANS AFFAIRS
WASHINGTON

March 3, 2026

Ms. Candace N. Wright
Director
Science, Technology Assessment, and Analytics
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Wright:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report: ***Artificial Intelligence Acquisitions: Agencies Should Collect and Apply Lessons Learned to Improve Future Procurements*** (GAO-26-107859).

The enclosure contains the action plan to address the draft report recommendation. VA appreciates the opportunity to comment on your draft report.

Sincerely,

A handwritten signature in black ink, appearing to read "Curt Cashour".

Curt Cashour
Chief of Staff

Enclosure

**Appendix V: Comments from the Department
of Veterans Affairs**

Enclosure

The Department of Veterans Affairs' (VA) Comment to the
Government Accountability Office (GAO) Draft Report
***Artificial Intelligence Acquisitions: Agencies Should Collect and Apply Lessons
Learned to Improve Future Procurements***
(GAO-26-107859)

Recommendation 4: The Secretary of Veterans Affairs should ensure that the Principal Executive Director of the Office of Acquisition, Logistics, and Construction (OALC) updates the Department's policies to establish processes and require officials to systematically collect lessons learned from AI Acquisitions--including best practices involving contract clauses--and submit them to GSA managed repository to enable sharing and application by other agencies.

VA Response: Concur. The Office of Acquisition, Logistics, and Construction (OALC) will coordinate with all stakeholders to identify processes to systematically collect lessons learned from artificial intelligence (AI) acquisitions. After identifying VA processes, OALC will update its policies and coordinate changes to any other related VA policies to detail the specific data requirements, information, and timeframes for lessons learned from AI acquisitions to be uploaded to the General Service Administration managed repository.

Target Completion Date: August 1, 2026

Appendix VI: GAO Contacts and Staff Acknowledgments

GAO Contacts

William Russell, RussellW@gao.gov

Candice N. Wright, WrightC@gao.gov

Staff Acknowledgments

In addition to the contact listed above, Nathan Tranquilli (Assistant Director), Holly Williams (Analyst-in-Charge), Kyra Chan, Sean Manzano, and William Reed made key contributions to this report. Other contributors included Vinayak Balasubramanian, Lorraine Ettaro, Lori Fields, Laura Greifner, Chris Pecora, and Alyssa Weir.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [X](#), [LinkedIn](#), [Instagram](#), and [YouTube](#).
Subscribe to our [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

<https://www.gao.gov/about/contact-us>



Agencies Should Collect and Apply Lessons Learned to Improve Future Procurements

GAO-26-107859

April 2026

A report to congressional requesters

For more information, contact: William Russell at RussellW@gao.gov or Candice N. Wright at WrightC@gao.gov.

What GAO Found

Federal agencies reportedly more than doubled their use of artificial intelligence (AI) from 2023 to 2024, and they used a range of approaches to acquire additional AI capabilities through fiscal year 2025. GAO identified trade-offs facing agencies as they acquire AI, and some associated challenges and benefits. For example:

- **Agency-directed vs. vendor-driven approaches.** Some agencies awarded new contracts in pursuit of AI solutions. In other instances, industry introduced capabilities to agencies in the absence of specific AI requirements.
- **Contracts vs. other agreements.** Agencies used different types of contracts to acquire AI capabilities. In some instances, agencies also leveraged other agreements not governed by federal acquisition regulations to develop more advanced AI capabilities.
- **AI as a service vs. a product.** Some agencies bought AI as a product, such as software. However, agency officials told GAO they acquire AI as a service where the vendor provides AI capabilities and outputs on an ongoing basis.

GAO identified several strategic and programmatic challenges agencies faced when acquiring AI capabilities.

Key Procurement Challenge Areas Identified by Selected Agencies

Strategic	Programmatic
Access to subject matter experts	Requirements definition and contract terms
Protections for government data and intellectual property rights	Early testing and continuous evaluation
Traditional acquisition timeframes and contract approaches	Artificial intelligence pricing and overall cost

Source: GAO analysis of interviews with agency officials from the General Services Administration and Departments of Commerce, Defense, Homeland Security, and Veterans Affairs. | GAO-26-107859

In April 2025, the Office of Management and Budget (OMB) issued guidance to help agencies acquire AI responsibly. OMB directed agencies to update their AI policies to comply with OMB's requirements. GAO previously reported that agency-level implementation is critical to achieving acquisition goals directed by OMB ([GAO-25-107398](#)).

In this review, GAO found the selected agencies were not yet systematically collecting lessons learned from AI acquisitions—a necessary first step to share knowledge about AI acquisitions in accordance with OMB guidance. OMB has stated that agencies should share knowledge about AI acquisitions through a web-based repository developed by the General Services Administration (GSA). However, officials at four agencies—GSA and the Departments of Defense (DOD), Homeland Security (DHS), and Veterans Affairs (VA)—told GAO they were not prepared to do so because their agency policies did not require them to collect lessons learned. As a result, the agencies are missing opportunities to identify and apply best practices—such as contract terms related to data rights or testing requirements—or to avoid mistakes as agencies increasingly acquire AI.

Why GAO Did This Study

Industry leads AI development, reportedly investing over \$250 billion in 2024 alone. Federal agencies are finding many opportunities to use AI to execute their missions. They already use AI for veteran services, enhancements to weapon systems, and administrative tasks. To realize the benefits of AI, federal agencies often contract with companies to acquire solutions. Members of Congress and others have raised concerns about federal AI acquisitions. These concerns include long-standing acquisition issues, such as fostering competition, as well as issues specific to AI, such as training AI models on flawed data.

GAO was asked to review federal AI acquisitions. This report addresses (1) acquisition approaches agencies are using to adopt AI, (2) types of challenges agencies face when acquiring AI capabilities, and (3) the extent to which selected agencies are prepared to share knowledge related to acquiring AI solutions.

GAO conducted in-depth reviews of 13 AI acquisitions at four federal agencies—DOD, DHS, GSA, and VA. GAO selected these agencies based on maturity of AI acquisition efforts and approaches to acquiring AI capabilities, among other factors. GAO reviewed the agencies' relevant policies, and interviewed senior AI acquisition leaders at the selected agencies. GAO also analyzed OMB guidance.

What GAO Recommends

GAO is making a total of four recommendations. Specifically, GAO is recommending that DOD, DHS, GSA, and VA update their policies to require officials to systematically collect lessons learned from AI acquisitions to enable sharing and application by other agencies. The agencies concurred with all of the recommendations.