



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 **[INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, 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_Notice_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 Pub. L. 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)