

April 3, 2026

The Honorable Edward Forst
Administrator
U.S. General Services Administration

Electronic Submission: maspmo@gsa.gov

Re: GSA General Services Acquisition Regulation Deviation 552.239-7001, *Basic Safeguarding of Artificial Intelligence Systems*.

Dear Administrator Forst,

The National Defense Industrial Association (NDIA) appreciates the opportunity to provide comments on the General Services Administration's (GSA's) General Services Acquisition Regulation (GSAR) Deviation 552.239-7001, *Basic Safeguarding of Artificial Intelligence Systems*.

NDIA is the nation's largest defense industry association, representing over 1,600 corporate and over 65,000 individual members from small, medium, and large contractors, a majority of which are small businesses. NDIA members design, manufacture, apply, and maintain the cutting-edge technologies, systems, and platforms that our armed forces rely upon to deter aggression and defend our nation and its interests. As such, our members' professional and informed views on this request for information reflect the complexity and nuance of the issues under discussion.

NDIA's member companies appreciate the GSA's efforts to establish a protective framework for artificial intelligence (AI) System use by creating General Services Acquisition Regulation (GSAR) Deviation 552.239-7001, *Basic Safeguarding of Artificial Intelligence Systems*. NDIA supports the Clause's overarching objectives – protecting Government data, encouraging the use of trusted AI capabilities, and ensuring the Government's use of AI for lawful purposes. NDIA also shares GSA's objective of establishing clear standards for responsible AI acquisition.

However, several provisions within the Clause introduce significant impediments to the responsible adoption of competitive AI Systems by Government contractors and their Service Providers. The Administration has made clear, through OMB Memorandum M-25-22 (OMB M-25-22), Executive Order 14179, and related guidance, that federal agencies should prioritize AI innovation, reduce regulatory barriers to commercial AI adoption, and leverage the commercial marketplace to advance the United States's leadership in AI innovation. However, a Clause that effectively requires commercial AI providers to build and maintain a parallel, Government-only product distinct from their commercial products and a compliance architecture with bespoke data handling, supply chain certification, IP assignment and ownership, and content moderation requirements works against these objectives. It raises the cost and complexity of efforts to modernize technology within the federal Government,

discourages commercial AI providers from participating in the MAS schedule, and risks ceding the Government AI market to providers willing to accept noncommercial terms. For those commercial providers that continue to sell to the Government, it limits their ability to quickly deliver the latest models for Government use.

The intersection of intellectual property (IP) and data rights with AI Systems is still a nascent and largely unsettled area. Any new proposals impacting ownership and liabilities around AI Systems and their outputs require a thorough analysis. As such, NDIA would respectfully request an extension of when GSAR Deviation 552.239-7001 would take effect to at least 90 days following the final publication of the MAS terms of service. NDIA would also be happy to convene industry partners to discuss these proposals in more detail at your convenience.

The following recommendations are offered as constructive feedback to revise GSAR 552.239-7001 to better balance protecting Government interests while preserving access to responsible AI systems:

- (1) Align Requirements with Commercial Practice to Preserve Competition: The proposed license structure exceeds what is necessary for contract performance and risks discouraging commercial AI vendors from participating in federal acquisitions. Contrary to the Revolutionary Federal Acquisition Regulation (FAR) Overhaul's mandate, the proposed Clause would require vendors to restructure AI service offerings specifically for Government use, converting what is nominally a commercial acquisition into a de facto bespoke procurement.

Many of the Clause's requirements diverge from current commercial practices for software (e.g., incident reporting, feedback handling, data segregation, documentation requests, prohibitions on technologies creating vendor dependencies) and will frustrate statutory preferences for commercial products and services.¹ This could also prevent commercial companies from enforcing their contractual license rights, including collecting fees for excess use of a Cloud Service and/or AI model.

Further, these requirements will create additional administrative burdens that will ultimately lead to higher costs to the Government, particularly for those contractors with commercial customers who must segregate Government Data not subject to security restrictions from other customer data and also ensure that such Government Data is not used to train AI. Where full disclosure is impractical, the Government should accept independent third-party assessments, standardized attestations (System and Organization Controls (SOC)-style), or narrowly tailored information disclosures subject to strong confidentiality protections.

Requirements around intellectual property rights, such as change management, custom development, and model rights, and constraints on using government data for training, are in

¹ 41 U.S.C. §3307 (Dec. 27, 2021); 10 U.S.C. §3453 (Dec. 23, 2024).

tension with rapidly evolving AI technologies. These requirements will slow the deployment of new capabilities and should be negotiated by contracting officers on a per-acquisition or use-case scenario. The approach of defaulting to the most cumbersome requirements and permitting negotiation to remove these requirements creates a strong presumption that these requirements must apply. The Government should avoid requirements that, in aggregate, establish a Government acquisition policy for AI requiring specialty U.S. AI Systems for use by government contractors.

- (2) AI Service Providers Should Be Responsible for Their AI Systems: The obligation in Paragraph (c) that primes must ensure full compliance from any AI supplier or AI system being used as part of performance, even those not in direct privity, poses a significant risk. This will limit use and access to cutting-edge commercial models, deter emerging vendors, and expose prime contractors to flow-down liability that cannot be realistically enforced. The definition of “Service Provider” may create confusion on how other contractual flow-downs may or may not apply, such as DFARS 252.204-7012, when the AI Systems involve the flow of Government Data. Substantive compliance obligations should be imposed directly on AI Service Providers that control the relevant AI Systems, including their technical architecture, model behavior, and configurations, rather than shifting primary responsibility to prime contractors that lack contractual rights to control or have visibility into such technical matters. Prime contractors cannot compel third-party model providers to expose proprietary algorithmic processes, restructure commercial products, or maintain government-specific versions. The Clause imposes unbounded liability for entities with no contractual relationship, and it is fundamentally inconsistent with FAR 52.212-4(c)(2), which gives primes discretion to flow down minimal clauses in commercial contracts. GSA should evaluate the merits of a shared responsibility model instead of mandating that the prime is responsible for an AI Service Provider. Prime contractors should retain accountability for flow-down performance proportionate to the control they can reasonably exercise and should not bear sole liability for service provider noncompliance or decommissioning costs arising from Service Provider-controlled failures.

- a. The definition of “Service Provider” or this Clause, in general, should clarify contractor responsibilities with respect to how this and other cyber clauses flow down. This will also help clarify and strengthen paragraph (c) of the definition related to contractor responsibility.
- b. Additionally, the order of precedence in paragraph (b), which indicates that the Clause controls if it conflicts with any contractor commercial terms, conflicts with a long effort of the U.S. Federal Government to ease the burden of commercial companies seeking to support federal requirements. The inclusion of this Clause could violate Section 1824 of the National Defense Authorization Act for Fiscal Year 2026 (P.L. 119-60) titled “Limitation on Required Flowdown of Contract Clauses to Subcontractors Providing Commercial Products or Commercial Services” pertaining to Department of War orders off of GSA schedules. Paragraph (b)’s order of precedence is incompatible with the

concept of GSA MAS as a commercial vehicle. Additionally, paragraph (j) restricts negotiation to only four areas at the order level. Combined with the order of precedence provision, this creates non-negotiable terms. The order of precedence provision should be removed or revised to preserve contractors' ability to negotiate terms at the order level.

- (3) Distinguish Government Data from Contractor Data to ensure Contractors Own What They Create: The Clause's definition of "Government Data" encompasses Contractor Input Data and Output Data, consequently transferring ownership of certain Contractor data through the Clause's requirement that the Government will own all Government Data and Custom Developments. "Data Inputs" captures contractor-developed prompts, instructions, and configurations. The clause thus treats contractor intellectual property as government-owned data that cannot be reused and effectively requires custom, government-specific AI development vs. commercial solutions. It would create a significant barrier as contractors would be forced to maintain entirely separate systems for government work. NDIA is concerned that the requirement for transferring contractor rights in Government Data (including enhancements, improvements, or derivative works) to the Government upon creation is overly broad and could both discourage new entrants from bringing their commercial technologies and/or discourage some industry leaders from offering their most competitive and innovative solutions, potentially limiting access to cutting-edge AI capabilities or innovation. This transfer could potentially conflict with Defense Federal Acquisition Regulation Supplement (DFARS) Clauses 252.227-7989, 252.227-7993, and FAR 52.227-14, each of which do not transfer ownership (copyright) to the Government, as well as the requirements in 41 U.S.C §2302 and 10 U.S.C. §3771 prohibiting regulations which impair contractor enjoyment of copyrighted works created under a contract.

Paragraph (d) as written may create unintended risk by limiting the Contractor's ability to reuse internally developed methodologies, tools, models, or enhancements in future contracts or commercial applications. Paragraphs (d)(1) and (d)(5) prevent contractors from using generative AI solutions for other engagements, even where the contractor's work reflects general technical expertise without government confidential information. This framework is inconsistent with FAR 52.227-14's framework for distinguishing government vs. private funding, and it effectively converts privately funded improvements to government property simply because they occurred during contract performance. The Clause also raises potential concerns related to the commingling of intellectual property and funding sources. In practice, AI development frequently involves the use of existing contractor-owned algorithms, frameworks, training methods, and datasets that may be refined or expanded during contract performance. Without clear boundaries between contractor pre-existing intellectual property, contractor-funded enhancements, and Government-funded developments, there is a risk that contractor-developed capabilities could unintentionally become subject to Government ownership or broader rights than intended.

To mitigate this risk, contractors would need to implement strict version control, configuration management, and cost segregation practices to clearly demonstrate what was developed using

Government funding versus contractor or commercial funding sources. This could increase administrative burden and may discourage contractors from incorporating innovative proprietary capabilities into Government solutions.

- a. The Clause’s definitions and ownership language should be modified to clarify that Contractors retain ownership of Contractor Data, consistent with U.S. Government acquisition policy. The Clause could also specifically define “Government-Owned Data” to help differentiate and also ensure that the Contractor Data has a separate license to ensure that Contractor Data with restrictions (e.g., Limited Rights) retains those protections when used as Input Data or found in Output Data. NDIA also recommends that the Clause provide clearer distinctions between contractor background intellectual property and Government-funded deliverables, as well as guidance on how derivative improvements or mixed-funding developments should be treated. Clarification in these areas would help ensure both protection of Government interests and preservation of contractor innovation incentives.
- (4) Exclude Indirect Service Providers Not Handling Government Data: The proposed Clause effectively forces prime contractors to impose compliance obligations on all third-party AI Service Providers whose systems are used during GSA contract performance – directly or indirectly. For large companies that use hundreds of AI tools, this Clause creates expansive compliance challenges. The Clause’s policy aims can still be achieved by limiting coverage to AI Systems that: (i) process Government Data, (ii) are delivered or made available to the Government as part of contract performance, or (iii) are specifically contemplated by the contract statement of work. This revised scope preserves the use of common ancillary commercial tools (e.g., human resources, finance, and productivity software), providing “back office” administrative support, avoids burdens on tools that do not implicate Government data or deliverables, and ensures GSA contractors leverage commercial tools to drive efficiency and reduce cost.
- (5) Clarify “American AI System” and Include Buy-American-Style Exceptions: While an American AI Systems requirement is commendable, the Clause should define “American AI System” with specific and clear metrics (e.g., ownership/operational control, amount of development in the United States, company headquarters vs. geographic location) and incorporate a phased implementation period, recommended as a 180-day period, to allow contractors to transition existing Schedule task orders to compliant AI Systems. OMB M-25-22 frames the Administration’s policy to maximize American AI use, not an absolute prohibition. Thus, the Clause’s categorical prohibition goes significantly further than M-25-22 requires. Moreover, modern AI development involves open-source frameworks with global contributions. Open-source software (OSS), which is commonly made available free of charge via open-source software licenses, and the commensurate cost savings, would become entirely inaccessible to the U.S. Government. OSS licenses offer no opportunity to flow down this GSA clause, effectively requiring that all AI be purchased. For those programs currently using OSS AI, those contractors will be forced to undertake a potentially significant redesign to use

procured AI where the Service Provider will agree to the GSA clause, driving significant costs to the U.S. Government, including through requests for equitable adjustment. Another major potential impact is where dual-use commercial companies that serve domestic defense equities collaborate with allied engineers (Five EYES, NATO) on their commercial products. This new requirement could be read to exclude those engineers from providing any development in order to qualify as an “American system” even beyond the funding considerations you point out from the investment/Foreign Ownership, Control, or Influence (FOCI) lens.

- a. The clause should focus on entity-level control and data residency rather than component-level origin.
 - b. In addition, “controlled by non-U.S. entities” needs to be further defined and whether a U.S. AI company with significant investments from non-U.S. entities would be barred.
 - c. The Clause should also include narrowly tailored exceptions—consistent with FAR 25.103 and 25.202—when no adequate domestic alternative exists or when cost or public interest considerations justify an exception. Additionally, testing may be necessary against “non-American” products to identify gaps and vulnerabilities to protect our national interests. GSA should also give consideration to a waiver from engineers from our close allies and partners.
- (6) Clarify Equitable Adjustment Claims Costs and Decommissioning Costs: It is not clear within the proposed Clause if implementation will be immediate or if there will be consideration given to the costs to change existing systems and solutions to come into compliance with the Clause. There is a tremendous amount of additional burden in supply chain tracking and auditing required for implementation, which will add costs to the contractor. In addition to the recommended 180-day implementation timeline in Comment 5, GSA should clarify a contractor’s ability to file equitable adjustment claims associated with the new costs for compliance.
 - a. NDIA also recommends removing subparagraph (i)(3)(ii) referencing “decommissioning costs.” The contractor’s liability resulting in a termination for cause or termination for default is already outlined in FAR Part 12 and FAR Part 49, respectively. This guidance and applicable prescribed clauses were maintained in the RFO. Additional language in the proposed clause is unnecessary.
- (7) Align Change Management with Commercial Practices: Paragraph (h) of the draft Clause requires Service Providers to provide successor models for discontinued AI tools, notify the Government within seven calendar days of any service change that materially increases output bias or decreases safety guardrails, and provide at least 30 days’ advance written notice to the Contracting Officer prior to adding a new Service Provider or materially altering an existing Service Provider. These requirements are fundamentally incompatible with how the commercial AI services model works. AI services are developed and updated continuously,

often with rapid iteration cycles that cannot accommodate 30-day advance notice requirements for every material change to a Service Provider. Requiring Service Providers to provide successor models for all discontinued tools and to notify the Government of every safety guardrail change would inhibit the pace of AI innovation and impose administrative burdens that cannot be operationalized at scale across a large and diverse customer base.

- a. While considering timelines in paragraph (h) on Change Management, the Government should consider the potential for delays in deliverables in cases in which there is a need to switch suppliers or AI products mid-performance. Particularly when directed by the Government, providing a specific timeframe for transition exceptions in such cases could prevent schedule disruptions while maintaining compliance with government requirements.
- (8) Data Handling, Localization, and Deletion Obligations: Paragraph (d)(4) of the draft Clause would require Contractors and Service Providers to implement “eyes off” data handling procedures restricting human review of Government Data, comply with data localization requirements, maintain logical segregation of Government Data from non-Government customer data, and — upon contract expiration — securely delete all Government Data and any Custom Developments from all systems, backups, and derivatives, with written certification to the Contracting Officer.
- a. While industry supports robust data protection for Government customers, several of these requirements present significant operational challenges for many businesses. The mandatory deletion and certification obligation, applied across all systems, backups, and derivatives at scale, directly conflicts with how many Contractors handle data retention and backup management for commercial — and government — customers. Compliance with the Clause’s data handling, localization, and deletion obligations would impose substantial operational burdens and costs on many Contractors who hold MAS contracts.
 - b. NDIA requests that GSA conduct a review to determine the specific use cases where these additional requirements are necessary and to ensure that they align with existing cybersecurity data handling standards. Specifically, regarding paragraph (d)(4)(ii), we recommend that GSA consider a requirement to implement role-based access controls with logging and audit trails that permits limited human access to Government Data for authorized personnel for legitimate business purposes, including security monitoring, incident response, and system maintenance, rather than strictly requiring “eyes off” data handling procedures. With respect to paragraph (d)(4)(vi), we request that GSA provide reasonable timelines for deletion certification and clarify that the deletion obligation does not apply to anonymized or aggregated technical data that contains no Government usage context.
- (9) Ongoing Implementation of OMB AI Systems Directives: Paragraph (i)(1)(iii) would require Contractors to implement OMB directives related to AI Systems that are issued during the

contract term upon Government request, whether or not those OMB directives had been codified in statute or regulation. As written, this provision creates an open-ended compliance obligation for future, undefined requirements based on non-binding agency guidance that may emerge after contract award. And, if the OMB directives were not rooted in existing statute and/or regulation, the provision would inevitably create conflicts with Contractors' compliance obligations under existing statutes and/or regulations. The provision would impose operational challenges for Contractors with MAS contracts, who would be forced to tailor AI Systems for a small subset of Government customers in ways that the Government could unilaterally change at any time. Under the FAR, such a change in the scope of compliance obligations requires a bilateral modification. *See* FAR 43.103(a). Accordingly, we request that GSA limit this provision to apply only to those OMB directives related to unbiased AI principles that are based in statute and/or regulation and also update this provision to provide for a mutually agreed-upon, bilateral modification between the parties.

- (10) Continuous Improvement Process for AI System Trustworthiness and Content Compliance: Paragraph (i)(1)(ii) of the draft Clause requires prime Contractors to establish and maintain, through regular fact-based output verification, continuous improvement processes to detect and mitigate AI system issues including, in pertinent part, trustworthiness concerns, bias, and illegal or prohibited content generation. It is also unclear what "illegal" or prohibited" content means in this context, particularly when read in conjunction with the Government's request for rights to use the model for any lawful purpose.
- a. First, this requirement imposes obligations that extend beyond AI Contractors' standard commercial service terms by mandating Government-specific continuous improvement processes, fact-verification protocols, and content monitoring systems that commercial customers do not receive as part of standard service offerings. Additionally, Service Providers typically do not grant their customers (e.g., prime Contractors) the level of technical access, control, or modification rights necessary to independently establish and maintain any continuous improvement processes for the underlying AI systems. Thus, prime Contractors cannot comply with paragraph (i)(1)(ii) because even as direct AI systems providers, they cannot implement continuous improvement processes that fundamentally alter commercial AI models without creating Government-specific versions that diverge from commercial products and reduce the government's access to commercial innovation.
 - b. Where prime Contractors leverage AI Service Providers as part of their solutions provided to Government customers, prime Contractors also would not possess the requisite ownership rights, source code access, or operational control over third-party AI models and systems, to conduct the Clause's mandated fact-based output verification and implement the continuous improvement processes. Accordingly, we respectfully request that GSA remove the requirement to create Government-specific continuous improvement processes and instead defer to Contractors' and Service Providers' established commercial practices for AI system monitoring and quality assurance, which

have proven effective in addressing trustworthiness, bias mitigation, and content appropriateness across diverse industry applications. Additionally, GSA should clarify the meaning of “illegal” or “prohibited” content.

- (11) Ensure Output Data Respects Input Data Licensing: Although the Clause partially addresses IP rights, the Clause remains silent on the critical issue of data rights of the U.S. Government in Output Data when the U.S. Government has less than unlimited or unrestricted rights to Input Data. The Clause should be expanded to ensure that any IP and data rights license limitations for Input Data and training data are appropriately reflected in the Output Data (e.g., Output Data should be subject to limited rights where Input Data is subject to the same).
- (12) Permit Uses of Government Data to Support Government Missions: The Clause prohibits any use of Government Data to improve or train AI Systems, impeding critical use cases, such as training weapons systems to become more effective. The Clause should be updated to provide options for contracting officers to authorize Government-approved training uses—subject to safeguards—so mission-critical capabilities can be improved without invalidating commercial models or undermining provider relationships.
- (13) Define the Term “Discretionary” in Paragraph (d): As used in subparagraph (2) of paragraph (d), the term “discretionary” needs to be defined with sufficient precision so that Contractors and Service Providers have a clear and defensible standard. The Clause should confirm that output restrictions are non-discretionary when they are required by applicable law or regulation, security control baselines imposed by an authorizing official, program security plans, or other Government-directed security requirements, or AI risk management controls implemented in accordance with NIST AI Risk Management Framework (RMF) or equivalent recognized frameworks. This clarification would support the intent of this section while providing Contractors and Service Providers a defensible standard for maintaining mandatory or risk-based guardrails.
- (14) Permit Use of Sanitized Feedback for Improvements: Although the Clause contemplates Government feedback, the Clause does not explicitly provide the Contractor or Service Provider a license to use such feedback for the Government and further prohibits use of feedback containing Government Data or Government confidential information for system improvements or beyond contract performance. The Government should provide a narrow, non-exclusive license allowing use of aggregated/non-identifiable feedback for remediation and system improvements.

The Clause also indicates that the feedback is Government feedback to the Contractor or Service Provider, “regardless of whether such feedback is generated by ... the Contractor, the Service Provider” As with the definition of Government Data, if Government feedback includes contractor feedback, this feedback should be owned to be consistent with the Government data rights policies in DFARS Clause 252.227-7013/7014, FAR 52.227-14, and statutory protections in 41 U.S.C §2302 and 10 U.S.C. §3771, as also noted above. Instead, the

clause should ensure that the Government gets a license to the feedback sufficient for the Government to implement the feedback in the AI system.

Additionally, the Clause uses the term “confidential”, which is a security classification subject to special treatment under Part 117 of 32 CFR (NISPOM). If the intent is that Government Data that has Controlled Unclassified Information (CUI), the Clause should replace references to “confidential” with CUI to prevent confusion with Government security levels, or provide a separate definition as to what constitutes Government confidential information.

- (15) Clarify Demonstrations of Bias Mitigation and Truthfulness: The clause leaves key terms undefined, including “ideological dogmas” and “partisan,” which creates subjective compliance risk. Contractors cannot independently verify compliance against undefined and subjective standards. For the Unbiased AI Principles, the Clause should provide clear, measurable, and objective standards or processes for an AI Service Provider to establish a lack of bias in an AI System. In addition to disclosed standards, GSA should adopt a collaborative evaluation framework through which government customers would benchmark AI systems upfront against disclosed standards, share assessment results with contractors, and then work collaboratively to address gaps. Once validated, contractors should not be subject to ongoing decommissioning liability.
- (16) Narrow and Clarify Contractor Disclosure Requirements: The disclosure requirements in paragraph (e)(1) are overly burdensome as AI is increasingly embedded in many software tools, including common office applications, often in ways that are not apparent. Broad disclosure mandates could disproportionately impact defense contractors and small businesses. NDIA recommends scoping this requirement narrowly to focus on AI systems explicitly developed, modified, or procured for contract performance and excluding common off-the-shelf software with incidental AI capabilities. This is an example of where compliance obligations may increase costs and compliance risks for all. Attempting to comply with such far-reaching and burdensome requirements slows down procurements and innovation while driving up costs.
 - a. Additionally, NDIA would ask GSA to clarify whether the requirements for reporting, including the 30-day notification under paragraph (e)(1), will be retroactively applied to existing contracts when this Clause is added. Explicit timelines and phased guidance for transitioning active contracts would minimize operational delays and ensure adherence to the new requirements without causing performance disruptions.
- (17) Harmonize Incident Reporting and Documentation Requirements: The Clause’s mandatory, non-negotiable requirements in paragraph (e), including extensive documentation of AI decisions, human oversight mechanisms, traceability, and 72-hour incident reporting, create substantial operational overhead. The incident reporting requirements in paragraph (e)(4) may impose additional burdens on certain contractors who already have reporting obligations under existing contracts with the Department of War (e.g., DFARS) or for AI systems used in

classified contracts. It could also inadvertently strain resources during critical moments by creating duplicative reporting requirements, which may hinder timely responses to incidents. To address this, it is recommended to harmonize this section by explicitly stating that reporting under DFARS satisfies this requirement or that reporting under the Cybersecurity and Infrastructure Security Agency (CISA) fulfills the cyber incident reporting obligations under DFARS. Additionally, the Clause should include guidance on reporting AI-related incidents involving classified data (e.g., specifying that such reporting is governed by applicable program security plans). This harmonization aligns with President Trump's "Cyber Strategy for America" (March 2026), Pillar 2's commitment to streamline cybersecurity regulations and reduce duplicative compliance burdens.

- a. Unbiased AI is used in paragraphs (e)(6)(C) and (E) is not defined. This leads to a vague and subjective standard, which increases the risk for performance disputes. These requirements should be harmonized with the NIST AI Framework—particularly 2.11 on fairness and bias as identified in the MAP function—as it requires fairness and bias to be evaluated, and results are documented.
 - b. Additionally, the breadth of documentation requirements under paragraph (e)(6) could deter new commercial companies from contracting with the Government, as they may view the requirements as disclosing their proprietary secrets on how AI is used to create, enhance, and adapt their products for various commercial markets.
- (18) Clarify Evaluation Benchmarks: Under paragraph (i)(2) "Government Evaluation Rights and Remediation," part ii relies on "Government benchmarks" as a cornerstone for testing and verification, yet these benchmarks have not been clearly defined or standardized. The draft Clause permits the Government to conduct automated assessments of AI systems at any time using its own benchmarks, without any obligation to disclose those benchmarks or methodologies. Additionally, for agentic, reasoning, or retrieval processes, the AI system must make intermediate steps, model routing decisions, and data retrieval methods accessible through audit trails. Without a concrete specification, contractors cannot effectively design or implement tools and interfaces that will align with the government's needs.
- a. Contractors' tools and interfaces may be proprietary, environment-specific, or dependent on technical stacks that differ from the government's existing tools or infrastructure. The government is requesting tools to test the contractor's AI system against benchmarks that are undefined, leading to a circular problem unless additional clarifications are provided. The contractor must have clear requirements to ensure compatibility and deliver solutions that meet the government's goals.
 - b. NDIA supports the Government's goal of ensuring system benchmarks are met; however, testing directly in the production environment could create unintended risks, such as system outages, which may impact deliverables. To mitigate this, NDIA suggests conducting tests in a dedicated staging environment or through sandboxed interfaces that

replicate production conditions without affecting live operations. This approach minimizes disruption while achieving the Government's evaluation objectives.

NDIA and its membership appreciate the opportunity to provide comments and firmly appreciate the government's desire to promote a strong, dynamic, and robust defense industrial base. But, without substantial revision, the Clause will prevent the federal government from accessing the best American AI capabilities available in the commercial market. NDIA stands ready to engage in further dialogue to develop workable solutions. If you have any questions related to these comments, please reach out to Michael Seeds at mseeds@ndia.org.

Sincerely,

National Defense Industrial Association