BSA Comments on the Office of Management and Budget Request for Information on Responsible Procurement of Artificial Intelligence in Government
April 25, 2024

BSA | The Software Alliance (BSA) appreciates the opportunity to provide comments on the Office of Management and Budget's (OMB) Request for Information (RFI) on Responsible Procurement of Artificial Intelligence (AI) in Government.

BSA is the leading advocate for the global software industry.[1] BSA members are at the forefront of developing cutting-edge services — including AI — and their products are used by businesses across every sector of the economy.[2] For example, BSA members provide tools including cloud storage and data processing services, customer relationship management software, human resource management programs, identity management services, cybersecurity services, and collaboration software. BSA members are on the leading edge of providing AI-enabled products and services. BSA members have also supported the federal government's IT modernization efforts and have extensive experience providing software services, including AI, to the federal government. As a result, they have unique insights into the technology's tremendous potential to spur digital transformation and the policies that can best support the responsible use of AI.

BSA's views are informed by our experience working with member companies to develop the BSA Framework to Build Trust in AI,[3] a risk management framework we published almost three years ago to help companies mitigate the potential for unintended bias in AI systems. Built on a vast body of research and informed by the experience of leading AI developers, the BSA Framework outlines a lifecycle-based approach for performing impact assessments and highlights corresponding best practices.[4] Our experience on these issues informs our recommendations below.

---

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk, and Zoom Video Communications, Inc.

[2] *See* BSA | The Software Alliance, Artificial Intelligence in Every Sector, *available at* https://www.bsa.org/files/policy-filings/06132022bsaaieverysector.pdf.

[3] *See* BSA | The Software Alliance, Confronting Bias: BSA's Framework to Build Trust in AI, *available at* https://www.bsa.org/reports/confronting-bias-bsas-framework-to-build-trust-in-ai.

[4] BSA has testified before the United States Congress and the European Parliament on the Framework and its approach to mitigating AI-related risks. *See, e.g.,* Testimony of Victoria Espinel, Public Hearing on AI & Bias, Special Committee on Artificial Intelligence in a Digital Age, European Parliament, Nov. 30, 2021, *available at* https://www.europarl.europa.eu/cmsdata/244265/AIDA_Verbatim_30_November_2021_EN.pdf; Testimony of Victoria Espinel, The Need for Transparency in Artificial Intelligence, Before the Senate Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protection,

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

OMB's RFI seeks information to help align the federal government's AI procurement practices with the obligations established in OMB's AI M-memo on federal agencies' development and use of AI. At the outset, we highlight three key priorities for addressing AI procurement:

- **Using existing procurement methods.** The US government should employ existing procurement methods instead of creating AI-specific procurement regulations. This will create consistency in agency approaches, enable the acquisition workforce to apply existing rules to AI, and increase the timeliness of procuring products.

- **Avoiding fragmented agency implementation.** A standardized approach across agencies is necessary to avoid a single AI solution being subject to different authorization processes from different agencies. It will also avoid duplicative efforts by both federal acquisition staff and vendors.

- **Leveraging commercial solutions.** Commercial products are more effective than custom-built solutions in assisting agencies in streamlining and standardizing administrative processes and adapting quickly to change, including with respect to rapidly evolving technologies such as AI. Indeed, commercial technologies advance and improve faster than custom-built products for federal agencies. This is particularly true for AI, whether integrated into enterprise software services or offered as a stand-alone tool.

The RFI asks a range of specific questions, including how standard procurement practices can be used to best reflect emerging practices in AI procurement, strategies for promoting competition, and access to technical components of AI systems. Our response to several of these questions is included below, underscores the priorities outlined above, and highlights the following points:

- AI procurement should be treated similar to other technologies;
- Broad market participation and increased competition can be accomplished by using commercial products, large purchasing pools, and multi-cloud technology;
- Performance-based metrics should be included in RFPs rather than the FAR;
- OMB policies should recognize companies' interest in safeguarding proprietary information;
- Responsibilities for testing will vary based on the product or service; and
- OMB should prioritize agency implementation of the NIST AI Risk Management Framework (RMF).

I. Strengthening the AI Marketplace

Question 1: How may standard practices and strategies of Federal procurement, such as Statements of Objectives, Quality Assurance Surveillance Plans, modular contracts, use of contract incentives, and teaming agreements, as well as innovative procurement practices, such as those in the Periodic Table of Acquisition Innovations, be best used to reflect emerging practices in AI procurement? Are there

Product Safety, and Data Security, *available at* https://www.bsa.org/files/policy-filings/09122023aitestimonyoral.pdf.

additional materials or resources that OMB could provide to vendors or agencies to improve alignment between agency missions and technical requirements?

The Administration does not need to develop a separate method of procurement for AI. It should be treated like any other good or service or part of a good or service. Creating a separate procurement methodology would undermine the acquisition workforce's ability to leverage existing knowledge and processes to procure innovative solutions in a timely manner. While AI has unique aspects, it can be procured with the existing system and methods. Additions to federal procurement policy are not required to purchase this technology. Instead, the US government should focus on continuing to have more contracting officers, contracting representatives, and other contracting staff take the relevant technology-specific courses.

We note, however, that the OMB AI M-memo requires agencies to identify rights-impacting and safety-impacting uses of AI, which will likely affect a vendor's performance of a contract involving these uses. To facilitate consistency across agencies, OMB should prepare acquisition planning checklists and other guidance for agencies to identify safety- or rights-impacting uses of AI.

Response:

Question 2. How can OMB promote robust competition, attract new entrants, including small businesses, into the Federal marketplace, and avoid vendor lock-in across specific elements of the technology sector, including data collectors and labelers, model developers, infrastructure providers, and AI service providers? Are there ways OMB can address practices that limit competition, such as inappropriate tying, egress fees, and self-preferencing?

Response:

I. Commercial Technologies

The US government should vigorously enforce the statutory preference for commercial solutions and restrictions against tying to established technologies. Commercial solutions bring competition, which reduces vendor lock-in and barriers to entry, promotes innovation, and improves participation by small businesses.

II. Competition

BSA has concerns that any proposed limitation on the number of initial AI contractors that would go through the proposed FedRAMP Emerging Technology Framework would constrain the number of available contractors. As you know, in larger procurements, the use of down-selects is a common step that occurs throughout the procurement process, so that both the government and contractor can determine if they meet the requirements. BSA recommends that a large pool be created for AI needs so that individual contractors can compete on the AI rather than having a limited number of AI developers or deployers available. If the group of potential providers is limited, there will be a severe constraint on the companies that do not make the initial selection, thereby creating market "winners" and "losers" at time when the market is in flux.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

III. Use of Multi-Cloud to Create a Competitive AI Environment

The use of multi-cloud technology is an industry standard and a recognized best practice that the US government should use to make cloud computing more efficient, secure, and cost effective. Specifically, multi-cloud technology will enable federal agencies to work with multiple cloud service providers, rather than relying on a single infrastructure, platform, or software cloud, to leverage the breadth of innovation occurring across the cloud industry. This means that government agencies should not put all of their data in one cloud infrastructure, but rather leverage multiple cloud service providers' compute, analytics, AI, and other technologies.

A multi-cloud model allows agencies to distribute their applications, data, and workloads across different cloud environments while providing agency flexibility between providers. It allows for agencies to vary their use so that when emergencies occur, like hurricanes, fires, or the COVID-19 pandemic, the US government can quickly activate to address the challenge.

The adoption of multi-cloud technology also allows federal agencies to obtain the best value through robust competitive purchasing of industry-leading technology. When multiple cloud service providers are competing for the same work, the US government can take advantage of a competitive marketplace that encourages innovation and lower costs. Competition also prevents agencies from having "vendor lock-in" as multiple systems must be interoperable.

Question 3: Should the Federal Government standardize assessments for the benefits and trade-offs between in-house AI development, contracted AI development, licensing of AI-enabled software, and use of AI-enabled services? If so, how?

Response:

The Government should treat the procurement of AI like all other procurements, and focus on outcomes, not the technology type. AI could be part of the deliverable, but focusing too much on the specific type of technology takes focus away from a key priority – the overall capability and deliverable. The establishment of AI-specific approaches will hinder the procurement and adoption of the technology. Standardization is an important priority.

In addition, the Government should rely on commercial solutions to the maximum extent practicable. In-house production or contracts for the creation of new software with AI can lead to technical problems and increased risk. Custom-built technology solutions are often more expensive to maintain and quickly become outdated. Moreover, the FAR requires agencies to prioritize commercial solutions over custom-built alternatives. In short, licensing of AI-enabled software should follow standard commercial practices as is noted in FAR 12.212.

Question 4. How might metrics be developed and communicated to enable performance-based procurement of AI? What questions should agencies be asking vendors to determine whether AI is already being used in performance-based services contracts?

Response:

The use of metrics can be helpful in identifying appropriate benchmarks for performance-based outcomes. In lieu of establishing these metrics in the FAR, they can be communicated through a RFP for a specific contract, which provides sufficient flexibility for targeting specific use cases. It also enables the RFP to account for the diversity of AI products on the market.

II. Managing the Performance and Risks of AI

Question 5: What access to documentation, data, code, models, software, and other technical components might vendors provide to agencies to demonstrate compliance with the requirements established in the AI M-memo? What contract language would best effectuate this access, and is this best envisioned as a standard clause, or requirements-specific elements in a statement of work?

Response:

Access to documentation, data, code, models, software, and other technical components should remain the same as what is customarily provided in commercial transactions, and existing contract language suffices to address this issue. We understand the government's interest in gaining access to technical components of AI systems, particularly in light of the OMB AI M-memo's requirements for agencies to independently assess relevant documentation, but it is important that that objective be balanced against companies' legal and business interests in safeguarding proprietary information. In particular, it is critical to maintain the confidentiality of data used to train AI systems, which is an important proprietary business asset that is key to driving innovation. As an alternative to providing access to this sensitive information, companies can describe how they source the data and a summary of the type of data they use. In addition, code or software modeling is also sensitive proprietary business information and should be protected.

Further, companies may not always have access to the technical information the government is seeking. For example, companies may build upon open source models or third-party proprietary models and fine-tune the applications for integration into their own products. In these circumstances, they will not have access to certain information, including the training data.

Question 6: Which elements of testing, evaluation, and impact assessments are best conducted by the vendor, and which responsibilities should remain with the agencies?

Response:

The benefit of leveraging commercial AI solutions is that contract quality assurance is based on the "contractor's existing quality assurance systems as a substitute for Government inspection and testing before tender for acceptance unless customer market practices for the commercial product being acquired include in-process inspection." (see FAR 12.208). In this sense, the marketplace that is already using the product is a useful metric for quality assurance.

Further, the current market practices for testing and evaluation may vary depending on the product and the company's position in the AI supply chain. For example, if the company is merely providing an API connection to a third-party large language model (LLM), it would

not be able to provide the agency with the ability to test the model; that would be handled by the LLM. However, in other circumstances, companies can allow customers, including agencies, to fine tune models using their own data and provide tools for agencies to test models in their own environment. As a result, we recommend approaching this issue on a product-by-product basis.

Question 7: What if any terms should agencies include in contracts to protect the Federal Government's rights and access to its data, while maintaining protection of a vendor's intellectual property?

Agencies should not seek additional data rights that vary from commercial practices or that go beyond the requirements in the FAR's existing data rights clauses. For example, current practices and FAR clauses would not grant the government rights in data first produced outside of the performance of the contract, such as rights in AI training data, or rights in model improvements that are a part of commercial software provided under the terms of a commercial license. However, they would grant the government rights in certain data first produced in the performance of a contract, such as enriched data. There are no additional measures necessary to protect these government rights.

In addition, the OMB AI M-memo encourages agencies to consider contractual provisions that would prohibit the use of government data obtained in connection with the contract from being used to train or improve the functionality of commercial AI solutions without express permission from the agency. We encourage agencies to avoid the inclusion of such provisions because limiting the use of data – especially de-identified, disaggregated, or anonymized data – in an AI developer's product improvement process may be both inconsistent with commercial practices and limit innovation and future insights that could result from those improvements.

Questions 9: How might agencies structure their procurements to reduce the risk that an AI system or service they acquire may produce harmful or illegal content, such as fraudulent or deceptive content, or content that includes child sex abuse material or non-consensual intimate imagery?

Question 10: How might OMB ensure that agencies procure AI systems or services in a way that advances equitable outcomes and mitigates risks to privacy, civil rights, and civil liberties?

Response:

OMB's AI M-memo encourages agencies to use the NIST AI Risk Management Framework (RMF) to fill gaps, but it then outlines other risk management practices for agencies to implement. OMB should prioritize agencies' implementation of the RMF and encourage its use by organizations providing procured products and services to the government. The RMF identifies how organizations should incorporate trustworthiness characteristics, including fairness and management of harmful bias, into their risk management practices. It also enhances consistency among federal agency practices, as it provides a common language and framework for assessing risks. Notably, BSA's Framework to Build Trust in AI, mentioned above, explores in detail steps that companies can take to mitigate the risk of bias, including conducting bias testing and evaluating the representativeness of data.

* * *

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

Thank you for the opportunity to provide comments. We look forward to serving as a resource as you continue to consider AI policy issues.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org