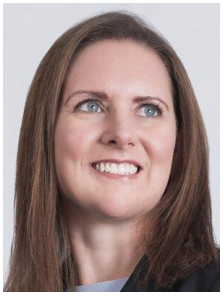
Gov't Contractors Should Prep For Increased AI Scrutiny

By **Tracye Howard, Kara Sacilotto and Lauren Johnson** (July 25, 2023)



Tracye Howard

Kara Sacilotto

Lauren Johnson

As artificial intelligence grows in popularity, discussion of its potential uses and risks is everywhere.

The U.S. Department of Defense is no exception and has been considering how AI development can be helpful or harmful to U.S. national defense.

In determining how to address certain concerns around the security and reliability of AI systems, the DOD is looking to broader cybersecurity measures that are growing in popularity, such as the software bill of materials, or SBOM.

Looking at the pattern of guidance and implementation of prior cybersecurity measures, government contractors and industry actors can draw from past lessons to help prepare for emerging guidance and requirements.

Department of Defense Initial AI Challenges

The DOD is currently pursuing AI projects that focus on three main areas: (1) recognizing targets through intelligence and surveillance analysis; (2) providing recommendations to operators on the battlefield, such as where to move troops; and (3) increasing the autonomy of uncrewed systems, such as aircraft and ships that do not require human operators.

The DOD and the U.S. Government Accountability Office have identified several challenges relating to the implementation of AI within the DOD.

One challenge is that training high-performing AI generally requires accurately labeled data — images, text files, videos, etc. that have been tagged with one or more identifiers — that the AI algorithm can learn from.[1]

Currently, most of the DOD's data is unlabeled. Because the process of labeling all previously gathered data would be too challenging and time-consuming, the most realistic solution is for the DOD to focus on incentivizing programs and contractors going forward to collect and store data in a standardized format that will be more usable by AI systems.

Another challenge the GAO identified is integrating AI into existing weapons platforms.

Because AI capabilities embedded in weapon platforms must be able to function in areas without access to digital infrastructure like the cloud, integration requires physical room for computing equipment that may not be available.

Thus, the DOD needs to understand the existing physical space capacity, and create the capacity needed within existing weapons platforms to enable the successful implementation of AI.

The Army's Approach to AI Challenges

Recognizing potential cybersecurity risks associated with AI systems, the U.S. Army is considering a new approach to identifying potential weak spots that could allow for malicious acts such as data poisoning — changing the data that AI systems rely upon — and backdoor or Trojan attacks, modifying an AI to function "normally" but given a specific input it will trigger an unintended act.

If implemented, the new approach would require companies seeking to provide AI products to the Army to turn over the underlying data and algorithms. The Army's experts would then review the algorithms to identify any areas that could potentially be targeted by bad actors or could otherwise threaten the ethical nature of the AI.

The Army does not want to accept a product without understanding how it works.

Companies may be reasonably concerned about turning over their algorithms.

Companies devote significant resources to developing and perfecting their algorithms and are likely not enthusiastic about providing those algorithms to a customer that could potentially reverse-engineer them, or allow a competitor to obtain access to them.[2]

The Army recognizes this concern and has emphasized that the goal of this potential effort is "not to get at vendor IP. It's really about, how do we manage the cyber risks and the vulnerabilities?"

Even so, the Army has acknowledged that it likely faces an uphill battle convincing companies to sign onto this approach.

Recognizing that private sector entities are essential to advancing DOD's AI initiatives, the Army has already started engaging with industry leaders to see how the parties can work together to make this effort work for both sides.

Lessons Learned From Software Bill of Materials

The Army's approach resembles the concept of a SBOM, a tool that has been under development in the private sector and government for years, though its use remains preliminary.

SBOMs have emerged as a promising tool to improve software security by creating supply chain transparency and allowing faster detection of new vulnerabilities.

President Joe Biden's 2021 Executive Order on Improving the Nation's Cybersecurity defines a SBOM as a "formal record containing the details and supply chain relationships of various components used in building software."[3]

As the Army and other government agencies consider how to identify the underlying data and coding of AI products, there are three lessons that can be learned from the process to date to refine and promote SBOM use.

First, the acceptance and adoption of SBOMs has grown in recent years as companies identified the long-term cybersecurity benefits.

Although software serves different functions depending on the industry, most companies recognize that software can be a vulnerability point for cyberattacks, whether directly or through the supply chain.

For example, the SolarWinds attack in 2019 emphasized the vulnerabilities in supply chain security and made many companies realize that they needed a way to identify what software components were integrated into their systems. But SBOMs are not a panacea — and AI BOMs will not be either.

Just as with SBOMs, government entities and contractors that may be asked to provide AI BOMs should understand exactly which risks can — and cannot — be addressed by disclosure of underlying data and processes used in AI products.[4]

Second, even with recent guidelines on what minimum elements should be included, information included in SBOMs varies between companies and can lack interoperability or scalability.

As the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response explained, despite growing industry adoption, SBOMs lack uniformity and there is no standard practice for what information most SBOMs should include.[5]

This lack of standardization continues despite the National Telecommunications and Information Administration's SBOM Minimum Elements Report, issued in 2021, which was developed in compliance with the Cyber EO.[6]

This problem could be compounded in the AI setting as large amounts of data are utilized and algorithms evolve. If AI BOMs are to succeed, baseline guidance that is flexible and provides minimum elements may help streamline adoption within the industry.

Third, while NTIA's guidance is voluntary, the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency is implementing a government-wide repository of software attestations from government contractors certifying adherence to a subset of the NTIA's minimum SBOM elements.[7]

Government contractors are often the first group to see the effects of federal cybersecurity priorities.[8]

The SBOM requirement is proving no different, and to the extent government contractors are required to provide AI BOMs, the broader AI industry could be getting a preview of how the federal government plans to handle some of the security risks that come with use of AI.

What to Know and What Actions to Take to Prepare for Evolving AI Requirements

Companies selling products and services to the government can take steps now to prepare for additional scrutiny of their technology and development practices, as well as more mandatory attestations and certifications.

Comply With Existing Guidance for Software

Several government bodies have already articulated guidance, which is still being finalized, for government contractors seeking to provide software.

For example, in September 2022, the Office of Management and Budget issued a guidance

memorandum[9] that requires agencies to obtain a self-attestation of compliance with the National Institute of Standards and Technology's Special Publication 800-218[10] from software producers before using their software.

This requirement applies to new software developed after Sept. 14, 2022, and major version changes to existing software after that date.

To implement this requirement, CISA developed a draft common form for self-attestation that, if approved by OMB, could be used by other government agencies to obtain the required self-attestations from software producers.[11]

Additional frameworks such as the NIST Cybersecurity Framework might also be modified to include supply chain and software development elements.[12] Contractors that have established systems and procedures for compliance with these software guidelines may have an easier time implementing similar obligations for AI development.

Take Advantage of Notice and Comment Opportunities

While different agencies have begun recommending AI policies, the Federal Acquisition Regulatory Council has not issued a rulemaking to govern AI use or procurement government-wide.

The council and the Defense Federal Acquisition Regulation Supplement do not currently regulate the procurement of AI separately from any other procured good or service.

The federal government has been procuring AI and AI-related systems and services for years, but without a rulemaking, agencies — and buying offices within agencies — are free to develop and implement separate requirements for each procurement that implicates AI.

Interested parties should be prepared to participate in the public notice and comment portion of any rulemaking or policy development that will govern sales of AI products and services to the government.

Similarly, as NIST and CISA develop specific guidance for development of AI, industry should join in the public commenting process.

Implement Guiding Principles

Although there are not yet any final rules or formal contractual obligations, government contractors and the AI industry generally, can look to the general guidance that has been issued by agencies and quasi-government bodies.

This guidance previews the factors that are most important to government actors and could likely be incorporated into final rulemakings or other AI requirements.

Such guiding principles, for example, can be found in the DOD's ethical principles[13] and the White House's Blueprint for an AI Bill of Rights.[14]

AI innovators should watch what the DOD does on bills of materials overall and for AI in particular.

As we have seen with cybersecurity over the past decade, and SBOMs in the past few years,

contractors often face the first set of meaningful obligations for new and emerging technologies, which may then proliferate across the broader innovation base.

Tracye Howard and Kara Sacilotto are partners, and Lauren Johnson is an associate, at Wiley Rein LLP.

Wiley partners Megan Brown and Duane Pozza, and Wiley associate Lisa Rechden, contributed to this article.

[1] U.S. Gov't Accountability Off., GAO-22-104765, Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon Systems (2022), https://www.gao.gov/products/gao-22-104765.

[2] John Prairie, Scott Felder, and Lisa Rechden, How Tech Firms Can Protect IP Rights on Federal Agency Contracts, Bloomberg Law (May 10, 2023), https://news.bloomberglaw.com/privacy-and-data-security/how-tech-firms-can-protect-ip-rights-on-federal-agency-contracts.

[3] Exec. Order No. 14028, 3 C.F.R. 26633 (2021).

[4] Christopher Bing, Chris Prentice, and Joseph Menn, Exclusive: Wide-ranging SolarWinds probe sparks fear in Corporate America, Reuters (Sept. 10, 2021), https://www.reuters.com/technology/exclusive-wide-ranging-solarwinds-probe-sparks-fear-corporate-america-2021-09-10/.

[5] Software Bill of Materials (SBOM) Sharing Lifecycle Report, U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (April 2023), https://www.cisa.gov/sites/default/files/2023-04/sbom-sharing-lifecycle-report_508.pdf.

[6] The Minimum Elements For a Software Bill of Materials (SBOM), National Telecommunications and Information Administration (July 12, 2021), https://ntia.gov/sites/default/files/publications/sbom_minimum_elements_report_0.pdf.

[7] Office of Management and Budget Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, (September 14, 2022) https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2022/sep/cs2022_0186.pdf.

[8] Megan Brown, Kara Sacilotto, and Tracye Howard, A New White House Project on Responsible AI Sends a Message to the Private Sector, Including Contractors, WileyConnect (May 31, 2023), https://www.wileyconnect.com/a-new-white-house-project-on-responsible-ai-sends-a-message-to-the-private-sector-including-contractors.

[9] Office of Management and Budget Memorandum M-22-18, Enhancing the Security of the

Software Supply Chain through Secure Software Development Practices, (September 14, 2022) https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2022/sep/cs2022_0186.pdf.

[10] Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities, N.I.S.T. Computer Security Resource Center, https://csrc.nist.gov/publications/detail/sp/800-218/final.

[11] Secure Software Development Attestation Form Instructions, Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/sites/default/files/2023-04/secure-software-self-attestation_common-form_508.pdf.

[12] NIST Cybersecurity Framework, National Institute of Standards and Technology, https://www.nist.gov/itl/smallbusinesscyber/planning-guides/nist-cybersecurity-framework.

[13] DOD Adopts Ethical Principles for Artificial Intelligence, U.S. Department of Defense (Feb. 24, 2020), https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.

[14] Blueprint for an AI Bill of Rights, White House Office of Science and Technology, https://www.whitehouse.gov/ostp/ai-bill-of-rights/.