DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY
ACQUISITION LOGISTICS AND TECHNOLOGY
103 ARMY PENTAGON
WASHINGTON, DC 20310-0103

SAAL-ZE

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Assistant Secretary of the Army (Acquisition, Logistics and Technology) Software Bill of Materials Policy

1. References. See enclosure.

2. Purpose. The purpose of this memorandum is to implement Army policy for the use of a Software Bill of Materials (SBOM) to enhance software supply chain risk management practices and effectively mitigate software supply chain risks.

3. Background. Issued on May 12, 2021, Presidential Executive Order 14028 (Improving the Nation's Cybersecurity) strengthens United States cybersecurity by focusing on modernizing federal government cybersecurity and improving the security of the software supply chain. The Office of Management and Budget (OMB) memorandum M-22-18 (Enhancing the Security of the Software Supply Chain through Secure Software Development Practices), 14 September 2022, required Federal agencies to comply with the National Institute of Standards and Technology (NIST) Secure Software Development Framework, SP 800-218 and the NIST Software Supply Chain Security Guidance OMB memorandum M-23-16 reinforces the requirements established in M-22-18 and provides supplemental guidance on the scope of M-22-18's requirements. Army Directive 2023-16 (Supply Chain Risk Management for Weapon Systems) states the original equipment manufacturers implement Supply Chain Risk Management (SCRM) during development and production, the Government has a shared responsibility to manage that risk. Software is a subset of SCRM risk and SCRM is to be conducted on systems throughout their lifecycle. Army Directive 2024-02 (Enabling Modern Software Development and Acquisition Practices) emphasizes the Army's reliance on software and the importance of understanding the risks systems can introduce to a network and how to mitigate those risks to the greatest extent possible.

4. Applicability: This policy applies to current and future programs planning to, or currently, executing on the Software Acquisition Pathway, Urgent Capability Acquisition, Middle Tier of Acquisition, Major Capability Acquisition, and Defense Business Systems.

5. Definitions.

a. SBOM is a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product.

b. For this policy, “covered computer software” refers to any computer software developed exclusively with Government funds to include Government-off-the-Shelf software, any computer software developed by a Contractor using exclusively Contractor funds or Independent Research and Development funds, any commercial computer software (as defined by FAR 2.101), and any noncommercial computer software developed and delivered to the Government by a Contractor. Commercial computer software includes Commercially off-the-shelf (COTS) software and open-source software.

c. “Covered Computer Software” does not include cloud services at this time.

6. Policy:

a. Program Executive Offices (PEO) and Program Managers (PM), as part of new contract actions, shall incorporate contract language requiring vendors to generate and deliver SBOMs for all covered computer software and SBOMs for COTS software where an SBOM is commercially available.

b. PEOs/PMs shall identify, in solicitations, the SBOM content to be delivered and the associated license rights needed by the Government. When an Offeror proposes lesser rights than the Government needs, PEOs/PMs shall negotiate for the necessary license rights as early as possible (preferably during contract negotiations), except in cases where negotiations would not be practicable.

c. PEOs/PMs shall collect SBOMs from vendors for covered computer software and SBOMs for COTS software where an SBOM is commercially available.

d. PEOs/PMs shall securely store and manage SBOMs in a PEO or PM-defined location.

e. PEOs/PMs shall monitor SBOMs throughout their portfolio and utilize them for vulnerability, incident management, and supply chain risk management in accordance with the SBOM Management and Implementation Guide.

7. Roles and Responsibilities:

a. Within 90 days from the date of this memorandum, the Deputy Assistant Secretary of the Army (Data, Engineering and Software) (DASA(DES)) will provide Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA(ALT) guidance and sample materials to include:

(1) Sample SBOM Contract Language.

(2) Sample Data Item Descriptions.

(3) SBOM Management and Implementation Guide.

b. Within 90 days from the date of this memorandum, DASA(DES) shall establish a cross-PEO/PM SBOM Working Group to gather policy implementation feedback, facilitate knowledge exchange, and promote collective problem solving.

c. Within 90 days of the release of guidance and sample materials from DASA(DES), PEOs/PMs shall:

(1) Collaborate with the Contracting Officer, as part of new contract actions, to incorporate SBOM contract language for covered computer software.

(2) Ensure that contract language(s) are passed on to subcontractors at all levels.

(3) Codify their processes for the collection, storage, management, and continuous monitoring of SBOMs in accordance with the ASA(ALT) SBOM Management and Implementation Guide.

(4) Codify their risk and incident management processes and procedures for risks and vulnerabilities uncovered through continuous monitoring of SBOMs in accordance with the ASA(ALT) SBOM Management and Implementation Guide.

d. Effective after 90 days of the release of guidance and sample materials from DASA(DES), PEOs/PMs shall:

(1) Collect and analyze SBOMs from covered computer software per ASA(ALT) SBOM Management and Implementation Guide.

(2) Perform SBOM collection, storage, management, and continuous monitoring of SBOMs in accordance with their codified processes.

(3) Perform risk and incident response activities in accordance with their codified processes.

(4) Periodically review and update their codified processes to reflect updates to ASA(ALT) SBOM Management and Implementation Guide.

(5) Periodically provide policy implementation feedback, share lessons learned, and participate in collective problem solving through the cross-PEO/PM SBOM Working Group.

8. Effective Date: This policy is effective immediately and stays in effect until superseded, rescinded, or incorporated into Army Regulation.

9. The Points of Contact:

a. DASA(DES) Policy Inbox: dasades@army.mil.

b. Mr. James Caseja, SBOM Team Lead at james.p.caseja2.civ@army.mil.

Bush.Douglas.R.9607501675 Digitally signed by Bush.Douglas.R.9607501675 Date: 2024.08.16 14:47:23 -04'00'

Encl

Douglas R. Bush
Assistant Secretary of the Army
(Acquisition, Logistics and Technology)

DISTRIBUTION:
ASSISTANT SECRETARY OF THE ARMY (ACQUISITION, LOGISTICS AND TECHNOLOGY) (SAAL-ZE, SAAL-ZF, SAAL-ZL, SAAL-ZN, SAAL-ZP, SAAL-ZR, SAAL-ZS, SAAL-ZT, SAAL-TE)
PROGRAM EXECUTIVE OFFICER:
ASSEMBLED CHEMICAL WEAPONS ALTERNATIVES
AVIATION
COMBAT SUPPORT AND COMBAT SERVICE SUPPORT
COMMAND, CONTROL, AND COMMUNICATIONS-TACTICAL
ENTERPRISE INFORMATION SYSTEMS
GROUND COMBAT SYSTEMS
INTELLIGENCE, ELECTRONIC WARFARE, AND SENSORS
MISSILES AND SPACE
SIMULATION, TRAINING, AND INSTRUMENTATION
SOLDIER
(CONT)

DISTRIBUTION: (CONT)
JOINT PROGRAM EXECUTIVE OFFICER:
ARMAMENTS AND AMMUNITION
CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR DEFENSE

DIRECTOR:
U.S. ARMY RAPID CAPABILITIES AND CRITICAL TECHNOLOGIES OFFICE
U.S. ARMY ACQUISITION SUPPORT CENTER

CF: ARMY CHIEF INFORMATION OFFICER

References:

a. Executive Order 14028 (Improving the Nation's Cybersecurity), 12 May 2021.

b. Office of Management and Budget Memorandum M-22-18 (Enhancing the Security of the Software Supply Chain through Secure Software Development Practices), 14 September 2022.

c. Office of Management and Budget Memorandum M-23-16 (Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices), 9 June 2023.

d. Secretary of the Army memorandum (Army Directive 2023-16 – Supply Chain Risk Management for Weapon Systems), 22 September 2023.

e. Secretary of the Army memorandum (Army Directive 2024-02 – Enabling Modern Software Development and Acquisition Practices), 11 March 2024.

f. National Institute of Standards and Technology Special Publication 800-161r1: Cybersecurity Supply Chain Risk Management for Systems and Organizations, May 2022.

g. National Institute of Standards and Technology Special Publication 800-218: Secure Software Development Framework, February 2022.

h. The Minimum Elements for a Software Bill of Materials, National Telecommunications and Information Administration, 12 July 2021.

i. Department of Defense Instruction 8500.01 (Cybersecurity).

j. Change 1, Implementation Guidance for Army Directive 2018-26 (Enabling Modernization through Management of Intellectual Property), 17 December 2020.

k. Federal Acquisition Regulation, 2.101 Definitions, 22 May 2024.