SECRETARY OF THE ARMY
WASHINGTON

22 SEP 2023

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Army Directive 2023-16 (Supply Chain Risk Management for Weapon Systems)

1. References. See references enclosed.

2. Purpose. This directive establishes policy and assigns responsibilities for conducting supply chain risk management (SCRM) for weapon systems to enhance the Army's ability to detect and manage supply chain threats and associated risks.

3. Applicability. The provisions of this directive apply to the Regular Army, Army National Guard/Army National Guard of the United States, and U.S. Army Reserve.

4. Policy. Army original equipment manufacturers and other industry partners are responsible for managing their supply chain during development through production, but the government has a shared responsibility to manage the risk.

a. SCRM is the process for managing risk by identifying, assessing, and mitigating threats, vulnerabilities, and disruptions to the Department of Defense supply chain, from beginning to end, to ensure mission effectiveness. Successful SCRM maintains the integrity of products, services, people, and technologies, and ensures the undisrupted flow of product, materiel, information, and finances throughout the life cycle of a weapon system. SCRM encompasses all subsets of risk, such as cybersecurity, software assurance, obsolescence, counterfeit parts, foreign ownership of sub-tier vendors, single points of failure (single-source producers), material sources, transportation, and other categories of risk that affect the supply chain pursuant to reference 1a.

b. SCRM will be conducted on systems throughout their life cycle. SCRM encompasses a system's mechanical, electrical, electro-mechanical, microelectronic, firmware, data, software, hardware, energetic compounds, and critical materials, as applicable.

c. Organizations will plan, program, budget, and execute funding for SCRM by balancing risk management with mitigations to ensure affordability.

d. System-specific supply chain vulnerabilities and risks will be protected at the appropriate security level determined by the organization's security manager and security classification guide.

e. Organizations conducting SCRM will leverage commercially available tools, standards, and best practices. A summary of high risks will be captured in the Life Cycle Sustainment Plan (sustainment risk section) or product support strategy.

f. SCRM compliance will be incorporated into sustainment reviews.

g. Policies for conducting cyber-SCRM on information, communication, and technology components, and for capturing the results in the Program Protection Plan, remain in effect pursuant to references 1g and 1h.

5. Responsibilities.

a. The Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA (ALT)) will—

(1) Develop SCRM policy for Army science and technology efforts and systems managed under the Defense Acquisition System, regardless of the system's Adaptive Acquisition Framework Pathway.

(2) Develop, publish, and maintain an Army SCRM guidebook that defines risk levels and provides detailed descriptions of SCRM processes and responsibilities.

(3) Ensure that program executive officers carry out SCRM requirements, including:

(a) conducting SCRM activities within the framework of identify, assess, mitigate, and monitor systems for which they oversee development

(b) developing funding requirements to support SCRM activities across systems for which they oversee development

(c) conducting SCRM assessments on systems for which they oversee development and documenting the results, capturing companies, suppliers, vendors, and distributors that pose the highest risk to the supply chain and the reasons why (detailing risk levels, acceptance authorities, residual risk levels, mitigations applied, risk categories, monitoring methods, and planned response actions to address emerging risks)

(4) Develop a long-term strategy to employ SCRM capabilities to identify, assess, and mitigate supply chain risks to current and future weapon system programs.

(5) Develop and publish procedures to promulgate SCRM lessons learned and mitigation strategies across the acquisition and sustainment communities. Forge relationships with industry, Department of Defense organizations, and other Federal agencies to adopt effective SCRM practices within the Army's SCRM capability.

(6) Develop and promulgate recommended contract statement of work language to support SCRM within the acquisition and sustainment communities. Take into consideration the inclusion of deliverables necessary to conduct SCRM, such as a bill of materials, original equipment manufacturer/vendor assessments, and notifications to materiel developers on supply risks/disruptions, including those tied to climate-change challenges.

(7) Ensure SCRM is conducted within a life-cycle framework of identify, assess, mitigate, and continuously monitor all systems. Take into consideration the need to document results.

b. The Commander, U.S. Army Futures Command (AFC) will establish procedures that maintain our competitive advantage by protecting science and technology overseen or executed by the U.S. Army Combat Capabilities Development Command (DEVCOM).

c. The Commander, U.S. Army Materiel Command (AMC) will—

(1) Manage the supply chain in sustainment, including the integration of SCRM into Army's sustainment enterprise management process.

(2) Ensure acquisition logisticians have the skills, knowledge, and abilities in supply chain risk management to provide the matrix support to program management organizations.

(3) Synchronize with the Defense Logistics Agency to ensure proper alignment with Army SCRM efforts and risk mitigation.

(4) Integrate the U.S. Army Contracting Command into the Army SCRM approach to ensure contracts contain statement of work language to support SCRM and establish oversight mechanisms that ensure compliance.

(5) Through the U.S. Army life-cycle management commands, partner with materiel developers during SCRM to formulate an understanding of the system's supply chain risk, mitigating actions, and monitoring requirements to effectively execute supply chain management at provisioning and throughout the system's life cycle until disposal.

d. The Deputy Chief of Staff, G-2 will:

(1) Collaborate and partner with stakeholders to develop an SCRM intelligence and security framework.

(2) Assist the Office of the ASA (ALT), AFC, and AMC in protecting mission-critical technologies, products, materials, and services by identifying and informing risk owners of foreign intelligence entity activities and any other adversarial attempts to compromise the Army's modernization and supply chain.

(3) Align Army intelligence and security enterprise assets and full-spectrum intelligence and security analytical support to supplement SCRM.

(4) Assist the Office of the ASA (ALT) in developing security statement of work language to support SCRM within the acquisition and sustainment communities.

(5) Provide counterintelligence and intelligence analytical support to materiel developers conducting SCRM.

(6) When requested by the Office of the ASA (ALT), represent Army in the Army SCRM Threat Assessment Center with the mission of conducting counterintelligence analysis of companies, suppliers, vendors, and distributors of components identified by materiel developers during SCRM.

6. Proponent. The ASA (ALT) is the proponent for this policy and will incorporate its provisions into a new Army regulation for SCRM within 2 years of the date of this directive.

7. Duration. This directive is rescinded on publication of the new regulation.

Christine E. Wormuth

Encl

DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
Commander
U.S. Army Forces Command
U.S. Army Training and Doctrine Command
(CONT)

DISTIBUTION: (CONT)
U.S. Army Materiel Command
U.S. Army Futures Command
U.S. Army Pacific
U.S. Army Europe and Africa
U.S. Army Central
U.S. Army North
U.S. Army South
U.S. Army Special Operations Command
Military Surface Deployment and Distribution Command
U.S. Army Space and Missile Defense Command/Army Strategic Command
U.S. Army Cyber Command
U.S. Army Medical Command
U.S. Army Intelligence and Security Command
U.S. Army Corps of Engineers
U.S. Army Military District of Washington
U.S. Army Test and Evaluation Command
U.S. Army Human Resources Command
U.S. Army Corrections Command
Superintendent, U.S. Military Academy
Commandant, U.S. Army War College
Director, U.S. Army Civilian Human Resources Agency
Executive Director, Military Postal Service Agency
Director, U.S. Army Criminal Investigation Division
Director, Civilian Protection Center of Excellence
Superintendent, Arlington National Cemetery
Director, U.S. Army Acquisition Support Center

CF:
Principal Cyber Advisor
Director of Enterprise Management
Commander, Eighth Army

REFERENCES

a. Department of Defense (DoD) Instruction 4140.01 (DoD Supply Chain Materiel Management Policy), 6 March 2019

b. DoD Instruction 4140.67 (DoD Counterfeit Prevention Policy), 26 April 2013, incorporating Change 3, effective 6 March 2020

c. DoD Instruction 4245.15 (Diminishing Manufacturing Sources and Material Shortages Management), 5 November 2020

d. DoD Instruction 5000.83 (Technology and Program Protection To Maintain Technological Advantage), 20 July 2020, incorporating Change 1, effective 21 May 2021

e. DoD Instruction 5000.90 (Cybersecurity for Acquisition Decisions and Program Managers), 31 December 2020

f. DoD Instruction 5010.44 (Intellectual Property (IP) Acquisition and Licensing), 16 October 2019

g. DoD Instruction 5200.44 (Protection of Mission Critical Functions To Achieve Trusted Systems and Networks (TSN)), 5 November 2012, incorporating Change 3, effective 15 October 2018

h. Army Regulation 70–77 (Program Protection), 8 June 2018

Enclosure