

VA CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT

1. **REASON FOR ISSUE:** This directive establishes the Department of Veterans Affairs (VA) Cyber-Supply Chain Risk Management (C-SCRM) policy pursuant to [Federal Acquisition Supply Chain Security Act \(FASCSA\) of 2018](#) and [Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure](#), issued on May 11, 2017. The C-SCRM policy is consistent with Federal and VA statutes, regulations, guidance, and policies listed in the References section.
2. **SUMMARY OF MAJOR CHANGES:** This is a new directive that establishes:
 - a. Overarching policy for managing risk derived from supplier-provided information, communication technology, and services (ICTS) products and services.
 - b. Roles and responsibilities among VA Administrations and Staff Offices.
3. **RESPONSIBLE OFFICE:** Office of Information and Technology (OIT) (005), Office of Information Security (OIS) (005R).
4. **RELATED DIRECTIVES and/or HANDBOOKS:** Not applicable.
5. **RESCISSION(S):** Not applicable.

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/

Paul R. Lawrence, Ph.D.
Deputy Secretary of Veterans Affairs,
Performing the Delegable Duties of the
Assistant Secretary for Information and
Technology and Chief Information Officer

DISTRIBUTION: Electronic Only

VA CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT

1. **PURPOSE.** This directive establishes the VA Cyber-Supply Risk Management (C-SCRM) policy. It communicates roles and responsibilities for managing cyber supply chain risks to VA, posed by information, communication technology, and services (ICTS) third-party vendors, supplies, and services.
2. **POLICY.**
 - a. Establish, implement and maintain a C-SCRM strategy and program to effectively manage ICTS supply chain risks associated with the development, acquisition, maintenance and disposal of systems, system components and system services and support [National Institute of Standards and Technology \(NIST\) Special Publication \(SP\) 800-53 Revision 5 \(Rev.5\)](#) Supply Chain Risk Management (SR) security controls in accordance with Federal requirements listed in the References section of this Directive.
 - b. Establish executive oversight and governance of C-SCRM program and practices.
 - c. Develop a Department-wide C-SCRM procurement process to evaluate potential suppliers and manage compliance and validity of approved suppliers and vendors.
 - d. Identify ICTS supplier base and maintain a list of suppliers critical to VA Missions.
 - e. Develop and maintain organizational C-SCRM requirements for suppliers.
 - f. Include C-SCRM requirements in all contracts with VA approved suppliers.
 - g. Require all ICTS acquisitions and decision-making processes incorporate and consider C-SCRM supplier risk assessments before, during, and after acquisition.
 - h. Establish an organizational cyber supply chain risk tolerance level consistent with the overall organizational risk tolerance level.
 - i. Integrate C-SCRM into System Development Life Cycle (SDLC) activities to ensure ICTS products and services are effectively evaluated and monitored throughout the lifecycle via the application of SCRM requirements to ICTS products and services.
 - j. Perform the activities in this C-SCRM directive across VA organizational tiers: Organizational, Business/Mission and Information Systems.
 - k. Monitor ICTS products and services for vulnerabilities within hardware, software and information assurance through rigorous test and evaluation capabilities, including developmental, acceptance and operational testing as required by [VA Directive 6500](#).
 - l. Share relevant cyber supply chain risk information to the Federal Acquisition Security Council's (FASC) Information Sharing Agency, Department of Homeland Security Cybersecurity and Infrastructure Agency (CISA), as well as with other Federal agencies as appropriate.

- m. Assess potential critical infrastructure, national security, and operational cyber-supply chain risks and impacts to the Department. Share identified risks with relevant VA stakeholders, including the Office of Operations, Security, and Preparedness (OSP) through the Integrated Operations Center, and other relevant Administrations and Staff Offices (A/SOs).
- n. Evaluate emerging foreign adversarial threats and trends targeting the cyber supply chain domain. Report all identified tactics, techniques, or otherwise indicators of compromise to internal stakeholders, including OSP through the Defensive Counterintelligence Program, and other relevant A/SOs.

3. RESPONSIBILITIES.

a. **Assistant Secretary for Information and Technology and Chief Information Officer (CIO)** must:

- (1) Advise the Secretary on C-SCRM matters and ensure VA is compliant with requirements under the Federal Acquisition Supply Chain Security Act (FASCSA) of 2018;
- (2) Designate a Senior Agency Official who will serve as the Chair of the C-SCRM Program Management Office;
- (3) Provide oversight for C-SCRM governance;
- (4) Ensure cyber supply chain risk assessments are prioritized based on the criticality of VA's mission functions, systems, components, services, or assets;
- (5) Oversee the development of the VA-wide C-SCRM strategy, implementation plan, policy, and process to guide and govern C-SCRM activities;
- (6) Coordinate with VA C-SCRM stakeholders to determine approved and prohibited technologies;
- (7) Integrate C-SCRM practices into the lifecycle of VA information systems, components, services or assets;
- (8) Share relevant cyber supply chain risk information to the Federal Acquisition Security Council's (FASC) Information Sharing Agency, the Department of Homeland Security Cybersecurity and Infrastructure Security Agency, as prescribed in the FASCSA of 2018;
- (9) Report on the progress and effectiveness of VA's C-SCRM program, as required by law, regulations, or policies;
- (10) Coordinate with the Principal Executive Director, Office of Acquisition, Logistics and Construction (OALC) to ensure that C-SCRM responsibilities are integrated into processes for VA acquisition programs, including research and development;

- (11) Direct and coordinate with VA Administration and Staff Offices to ensure that C-SCRM responsibilities are addressed throughout the agency;
 - (12) Integrate C-SCRM threat information sharing activities, both internal and external to the VA, to enhance VA cyber situational awareness;
 - (13) Establish agreements with suppliers to engage in cooperative C-SCRM activities;
 - (14) Ensure the VA C-SCRM program is continuously assessed and monitored; and
 - (15) Oversee the selection, tailoring and implementation of applicable VA C-SCRM security controls.
- b. **Deputy Chief Information Officer (DCIO) for Compliance, Risk, and Remediation (CRR)** must:
- (1) Ensure C-SCRM strategies and policies are aligned with overarching VA cybersecurity, privacy, and risk management strategies and VA business environments;
 - (2) Monitor and utilize all applicable VA assessed and cleared ICTS products and services lists; and
 - (3) Facilitate and/or conduct oversight in collaboration with OIT to ensure compliance, enforcement, coordination and training based on VA standards related to SCRM.
- c. **Executive Director, Office of Acquisition and Logistics (OAL) and the VA Senior Procurement Executive (SPE)** must:
- (1) In coordination with C-SCRM stakeholders, implement standardized policies and procedures to protect the integrity of the cyber supply chain system and provide comprehensive, strategic ICTS acquisition management support/services for complying with Federal mandates;
 - (2) Develop and maintain organizational C-SCRM requirements for suppliers;
 - (3) Coordinate with the Office of Information Technology (OIT) to ensure that C-SCRM responsibilities are integrated into processes for VA acquisition programs, including research and development; and
 - (4) Collaborate with OIT to develop a list of assessed and cleared ICTS products and services for distribution to other Federal agencies and/or organizations to include the FASC.
- d. **Deputy Assistant Secretary (DAS) for Information Security and Chief Information Security Officer (CISO)** must:
- (1) Develop and maintain C-SCRM requirements;

- (2) Ensure ICTS products and services are effectively evaluated and monitored throughout the system development lifecycle via the application of C-SCRM requirements;
- (3) Develop and implement a plan for managing supply chain risks associated with the development, acquisition, maintenance and disposal of systems, system components and system services;
- (4) Provide policy development, process engineering, risk management, compliance tracking, internal controls and audit processes;
- (5) Ensure the selection and implementation of ICTS C-SCRM cybersecurity controls for mitigation of cyber supply chain risk;
- (6) Identify and manage ICTS products and services from prohibited sources;
- (7) Assist in the development of acquisition solutions that support C-SCRM for use throughout VA;
- (8) Facilitate information sharing efforts between VA and Federal government and industry partners in support of C-SCRM, including threat and vulnerability information sharing;
- (9) Lead the development of policy, processes, procedures, controls, risk management, workflow, compliance tracking and internal control and assessments for suppliers to ensure compliance for information security, cybersecurity, privacy, acquisition and risk management of suppliers, contracts and acquisitions and category management for sourcing ICTS products and services;
- (10) Lead the development of policy, standards, procedures and controls stipulated in contractual terms, conditions and clauses for sourcing ICTS products and services by developing or procuring a record system and workflow to manage provenance, tracing verification and banned/approved product and supplier lists;
- (11) Coordinate, prioritize and support the execution of requests for threat analysis of suppliers of critical components;
- (12) Monitor ICTS products and services for vulnerabilities within hardware, software and information assurance;
- (13) Integrate C-SCRM into the existing VA Risk Management Framework (RMF);
- (14) Support the selection, tailoring and implementation of C-SCRM security controls;
- (15) Support the OSS with the development, tailoring and appropriate application of cybersecurity requirements to ICTS supplier contracts;

- (16) Support the development of security and privacy SCRM training and awareness products and a distributive training capability; and
 - (17) Support a process to ensure that ICTS supply chain security risks are documented in Plans of Action and Milestones (POA&Ms) to be remediated in accordance with VA policy.
- e. **Deputy Chief Information Officer (DCIO), Office of Strategic Sourcing (OSS)** must:
- (1) Assist in developing and maintaining organizational C-SCRM requirements for ICTS suppliers;
 - (2) Ensure the development and implementation of standardized guidance by supplementing the Federal Acquisition Regulation (FAR) and updating VA logistics and internal procedures, guidance and instructions as needed;
 - (3) Coordinate with the Contracting Officers (CO) to support enterprise risk management reporting of ICTS suppliers, supplies and services and corresponding security statuses;
 - (4) Development, tailoring and appropriate application of cybersecurity requirements to ICTS supplier contracts; and
 - (5) Perform ICTS C-SCRM and supplier cyber risk management oversight and risk assurance reviews and audits across VA ICTS and for VA organizations contracting with ICTS suppliers to ensure compliance with policies, standards, external regulations and controls.
- f. **Deputy Chief Information Officer for Product Delivery Service** must:
- (1) Review ICTS software requests and manage the Technical Reference Model (TRM), which includes the Standards Profile and Product List; and
 - (2) Ensure the selection and implementation of C-SCRM cybersecurity controls and mitigating ICTS supply chain risk.
- g. **Chief of Operations, Security, and Preparedness** must:
- (1) Maintain situational awareness of all C-SCRM impacts to VA Critical Infrastructure, Operations, and Services;
 - (2) Establish VA Integrated Operations Center's information sharing responsibilities for C-SCRM concerns which meet VA Critical Information Requirements;
 - (3) Advise Assistant Secretaries, Under Secretaries, and other Key Officials on C-SCRM impacts to VA Contingency and Continuity of Operations;
 - (4) Liaise with relevant Federal Partners for information exchange and necessary support related to C-SCRM impacts on VA operations; and

(5) Further delegate or designate responsibilities as required.

h. Executive Director for Infrastructure Operations Services must:

- (1) Build standards to support the VA enterprise infrastructure, providing solutions for VA business service requirements and develop standards for hardware and software components;
- (2) Ensure the selection and implementation of C-SCRM cybersecurity controls and mitigating ICTS supply chain risk; and
- (3) Review ICTS hardware-related requirements and requests, as part of Infrastructure Operations solution delivery and provide requirements and standards-based engineering solutions for VA enterprise infrastructure service requests.

i. Contracting Officers (CO) must:

- (1) Ensure the audit and enforcement of policies, standards and requirements specified in ICTS supplier contracts;
- (2) In coordination with system owners and the C-SCRM Program, ensure supplier cyber-supply chain risk assessments are completed prior to any ICTS contract award decision;
- (3) Ensure that solicitations and contracts include the appropriate information security and supply chain security requirements, as noted in VA Directive 6500, VA Handbook 6500.6 and other associated Handbooks;
- (4) Support continuous monitoring, ongoing awareness and enterprise risk management reporting of ICTS suppliers, supplies and services and corresponding security statuses; and
- (5) Ensure that contracts for services involving access to or disclosure of personally identifiable information (PII) have appropriate Federal Acquisition Regulation and VA Acquisition Regulatory privacy language.

j. Under Secretaries, Assistant Secretaries, and Other Key Officials must:

- (1) Ensure compliance with this directive;
- (2) Ensure all VA IT services and/or products that their respective organization manages, including biomedical assets (medical devices) and SaaS-enabled products, that connect to any VA network, are subject to rules, standards and oversight requirements as prescribed in this directive and other applicable policy;
- (3) Maximize collaboration with the C-SCRM community;
- (4) Plan, program and budget for VA IT services and/or products to ensure they are supportive of VA Administration and Staff Office requirements;

- (5) Ensure all personnel conform to C-SCRM requirements for all ICTS procurements; and
- (6) Ensure compliance of OMB M-23-16 and M-22-18, "Enhancing the Security of the Software Supply Chain through Secure Software Development Practices" as outlined by OMB Memoranda and Executive Orders.

4. REFERENCES.

a. Statutes and Regulations.

- (1) [S. 3085 – 115th Congress \(2017-2018\), Federal Acquisition Supply Chain Security Act of 2018](#)
- (2) [Federal Acquisition Regulation \(FAR\)](#)
- (3) [FAR Part 24, Protection of Privacy and Freedom of Information](#)
- (4) [FAR Part 40, Information Security and Supply Chain Security](#)
- (5) [FITARA - Pub. L. 133-291. The Federal Information Technology Acquisition Reform Act](#)
- (6) [John S. McCain National Defense Authorization Act for Fiscal Year 2019 Section 889\(a\)\(1\)\(A\)](#)
- (7) [Public Law 117-302, Strengthening VA Cybersecurity Act of 2022](#)

b. Executive Orders

- (1) [Executive Order 13636, Improving Critical Infrastructure Cybersecurity](#)
- (2) [Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure](#)
- (3) [Executive Order 14028, Improving the Nation's Cybersecurity](#)

c. National Institute of Standards and Technology (NIST)

- (1) [NIST Cyber Security Framework, Framework for Improving Critical Infrastructure Cybersecurity Version 1.1](#)
- (2) [NIST Interagency Report \(IR\) 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry](#)
- (3) [NIST SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations](#)
- (4) [NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations](#)

- (5) [NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*](#)

d. VA Policy

- (1) [VA Acquisition Regulation \(VAAR\)](#)
- (2) [VA Directive 6500, *VA Cybersecurity Program*](#)
- (3) [VA Handbook 6500, *Risk Management Framework for VA Information Systems: VA Information Security Program*](#)
- (4) [VA Handbook 6500.6, *Contract Security*](#)
- (5) [VA Directive 6008, *Acquisition and Management of VA Information Technology Resources*](#)
- (6) [VA Directive 6004, *Configuration, Change and Release Management Programs*](#)
- (7) [VA Directive 6403, *Software Asset Management*](#)

e. Other Directives and References

- (1) [CNSSD 505, *Supply Chain Risk Management, 26 July 2017*](#)
- (2) [Office of Management and Budget \(OMB\) Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*](#)
- (3) [OMB Memorandum M-23-16, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*](#)

5. DEFINITIONS.

- a. **Cybersecurity Supply Chain Risk Management (C-SCRM):** Process of identifying, assessing and mitigating the risks associated with the distributed and interconnected nature of IT/OT product and service supply chains. It covers the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage. SOURCE: [S.3085 - Federal Acquisition Supply Chain Security Act of 2018](#)
- b. **Critical Component:** Any component which is or contains ICTS, including hardware, software and firmware, whether custom, commercial or otherwise developed and which delivers or protects mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system. SOURCE: [Department of Defense Issuances \(DoDI\) 5200.44](#)

- c. **Federal Acquisition Regulation (FAR):** System established for the codification and publication of uniform policies and procedures for acquisition by all executive agencies. SOURCE: [NIST SP 800-161](#)
- d. **Federal Acquisition Supply Chain Security Act of 2018 (FASCSA):** An Act which establishes a Federal Acquisition Security Council and provides executive agencies with authorities relating to mitigating supply chain risks in the procurement of information technology and for other purposes. SOURCE: [S.3085 - Federal Acquisition Supply Chain Security Act of 2018](#)
- e. **Cyber Supply Chain:** Linked set of resources and processes between acquirers, integrators and suppliers that begins with the design of ICT products and services and extends through development, sourcing, manufacturing, handling and delivery of ICT products and services to the acquirer. Note: A cyber supply chain can include vendors, manufacturing facilities, logistics providers, distribution centers, distributors, wholesalers and other organizations involved in the manufacturing, processing, design and development, handling and delivery of the products or service providers involved in the operation, management and delivery of the services. SOURCE: [NIST SP 800-161](#)
- f. **Procurement:** Includes all stages of the process of acquiring products or services, beginning with the process of determining the need for the product or service and ending with contract completion and closeout. SOURCE: [NIST SP 800-161](#)
- g. **Prohibited Systems:** Software, hardware and services from suppliers banned by Federal decree. SOURCE: [NIST SP 800-161](#) Appendix E
- h. **Supply Chain Risk:** The risk that an adversary may sabotage, maliciously introduce unwanted functions or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation or maintenance of an item of supply or a system to surveil, deny, disrupt or otherwise degrade the function, use or operation of a system. SOURCE: [CNSSI 4009](#)
- i. **Supply Chain Risk Management (SCRM):** A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplies product and its subcomponents or the supply chain (for example, initial production, packaging, handling, storage, transport, mission operation and disposal). SOURCE: [CNSSI 4009](#)