UNITED STATES DEPARTMENT OF COMMERCE
Office of the Chief Financial Officer and
Assistant Secretary for Administration
Washington, D.C. 20230

PROCUREMENT MEMORANDUM 2015-08 (REVISED FEBRUARY 2025)

ACTION

MEMORANDUM FOR: Senior Bureau Procurement Officials and Chief Information Officers

FROM: Olivia J. Bradley
Senior Procurement Executive and
Director for Acquisition Management

OLIVIA BRADLEY Digitally signed by OLIVIA BRADLEY Date: 2025.02.20 14:30:07 -05'00'

Brian Epley
Chief Information Officer

BRIAN EPLEY Digitally signed by BRIAN EPLEY Date: 2025.03.04 10:22:02 -05'00'

SUBJECT: Supply Chain Risk Assessment (SCRA) Requirements for the Acquisition of Moderate-Impact and High-Impact Information Systems

1. Purpose

The purpose of this Procurement Memorandum is to provide Department of Commerce (Department)-wide direction to contracting officers and purchase card holders to implement the supply chain risk assessment requirements for the acquisition of new[1] FIPS-199 moderate-impact and high-impact information systems set forth in Section 514 of the Consolidated and Further Continuing Appropriations Act, 2024, and subsequent acts[2] and the Department's Cybersecurity Supply Chain Risk Management (C-SCRM) Handbook.[3] This policy is revised to update assessment procedures and references to relevant legislation.

2. Background

Information Technology (IT) relies on a global supply chain. This introduces multiple risks to federal IT, including a growing dependence on foreign technology, reduction of transparency and traceability of the supply chain through multinational mergers and acquisitions of suppliers and integrators, the potential exploitation of information through counterfeit materials and malicious software, and reliance upon malicious or unqualified service providers for the performance of technical services.

Section 514 of the Consolidated Appropriations Act, 2024 states:[4]

(a) None of the funds appropriated or otherwise made available under this Act may be used by the Departments of Commerce and Justice, the National Aeronautics and Space Administration, or the National Science Foundation to acquire a high-impact or moderate-impact information system, as defined for security categorization in the National Institute of Standards and Technology's (NIST) Federal Information Processing Standard Publication 199,

[1] A new procurement is associated with a high- or moderate-impact system as defined by the security categorization process in accordance with FIPS 199, subject to the reporting requirements of 44 U.S.C. Section 3505, and for which either: (1) a new system inventory record will be entered in CSAM; or (2) the system undergoes a significant change as defined by the Configuration Management Standard.

[2] Hereinafter referred to as "appropriated funds."

[3] The handbook can be found in the IT Policy Library under the DOC Enterprise Cybersecurity Policy Program or at https://connection.commerce.gov/sites/default/files/media/files/2024/cybersecurity_supply_chain_risk_management_handbook_v1.0_2.28.24_rr.pdf

[4] This language was in Section 515 of the Consolidated and Further Continuing Appropriations Act, 2015, and in Section 514 starting in fiscal year 2018 and subsequent acts.

'Standards for Security Categorization of Federal Information and Information Systems' unless the agency has—

(1) reviewed the supply chain risk for the information systems against criteria developed by NIST and the Federal Bureau of Investigation (FBI) to inform acquisition decisions for high-impact and moderate-impact information systems within the Federal Government;
(2) reviewed the supply chain risk from the presumptive awardee against available and relevant threat information provided by the FBI and other appropriate agencies; and
(3) in consultation with the FBI or other appropriate Federal entity, conducted an assessment of any risk of cyber-espionage or sabotage associated with the acquisition of such system, including any risk associated with such system being produced, manufactured, or assembled by one or more entities identified by the United States Government as posing a cyber threat, including but not limited to, those that may be owned, directed, or subsidized by the People's Republic of China, the Islamic Republic of Iran, the Democratic People's Republic of Korea, or the Russian Federation.

(b) None of the funds appropriated or otherwise made available under this Act may be used to acquire a high-impact or moderate-impact information system reviewed and assessed under subsection (a) unless the head of the assessing entity described in subsection (a) has--
(1) developed, in consultation with NIST, the FBI, and supply chain risk management experts, a mitigation strategy for any identified risks;
(2) determined in consultation with NIST and the FBI that the acquisition of such system is in the national interest of the United States; and
(3) reported that determination to the Committees on Appropriations of the House of Representatives and the Senate and the agency Inspector General.

3. Supply Chain Risk Assessment

Supply Chain Risk Assessment (SCRA) is the process by which the Department of Commerce's Supply Chain Risk Management Program (SCRMP) conducts a thorough review of new[5] FIPS 199 high-impact and moderate-impact information systems for potential cyber-espionage or sabotage risks, including an assessment of the presumptive awardee(s) against available and relevant threat information as outlined in the Standard Operating Procedure for Supply Chain Risk Assessments for the Acquisition of Moderate-Impact and High-Impact Information Systems.[6]

No federal funds may be used to acquire a new FIPS 199 high-impact or moderate-impact information system unless an SCRA is completed, ensuring that supply chain risk is identified, and the acquisition aligns with the national interest.

[5] A new procurement is associated with a high or moderate impact system as defined by the security categorization process in accordance with FIPS 199, subject to the reporting requirements of 44 U.S.C. Section 3505, and for which either: (1) a new system inventory record will be entered in CSAM; or (2) an existing inventory record will be modified in CSAM.

[6] The most current standard operating procedures can be found on the Department of Commerce Supply Chain Risk Management Program (SCRMP) intranet page.

4. Required Actions

Effective immediately, the program office shall submit all new[7] purchase requests for IT[8] using funds appropriated or otherwise made available by appropriated funds including requests below the micro-purchase threshold, to the cognizant Chief Information Officer (CIO) or designated representative[9] with a completed Department of Commerce Office of the Chief Information Officer's IT Compliance in Acquisition Checklist (IT Checklist). The checklist will inform the cognizant CIO or designated representative whether the acquisition is subject to an SCRA. The cognizant CIO or designated representative may also require an SCRA for an acquisition at their discretion.

a. If the cognizant CIO or designated representative determines, based on the completed IT Checklist, that the acquisition requires an SCRA, the purchase request shall be referred to the servicing acquisition office for acquisition by a warranted contracting officer, even if it otherwise might have been procured via the purchase card.

   i. If the acquisition is subject to an SCRA, the contracting officer shall include the language provided in Section 5 below in the solicitation and resulting contract. If the acquisition is under an existing contract (e.g., an indefinite-delivery, indefinite-quantity contract), the contracting officer shall modify the contract to include the language in Section 5.
   ii. Upon completion of the review of initial proposals, the contracting officer shall mark and securely transmit the SCRA information from the offerors in the competitive range or the presumptive awardee to the cognizant CIO or designated representative and request an SCRA assessment. Such material shall be protected and marked as contractor bid or proposal information and source selection information in accordance with FAR 3.104-4.
   iii. The cognizant CIO or designated representative shall send the SCRMP a completed SCRMP SCRA intake form[10] via the current DOC Secure File Transfer (SFT) solution. Any requests for additional information from the offeror/contractor shall be coordinated through the contracting officer.
   iv. Using the information provided by the offeror/contractor, as well as additional analytical tools at its disposal, SCRMP shall conduct a comprehensive assessment of any risk of cyber-espionage or sabotage associated with the acquisition of such system, including any risk associated with such system being produced, manufactured, or assembled by one or more entities identified by the United States Government as posing a cyber threat, including but not limited to those that may be owned, directed, or subsidized by the People's Republic of China, the Islamic Republic of Iran, the Democratic People's Republic of Korea, or the Russian Federation. The SCRMP's completed assessment report shall be made available to the cognizant CIO or designated representative, Chief Information Security Officer (CISO), and designees.
   v. **Cognizant CIO Risk Assessment Determination**
   Following receipt of the completed SCRA report from SCRMP, the cognizant CIO or designated representative, in consultation with the Department's CIO, shall assess and determine whether

7 This includes purchase requests for new actions; not modifications for existing actions unless a checklist would otherwise be required. This also includes new orders under existing blanket purchase agreements or indefinite delivery, indefinite quantity contracts including those under existing strategic sourcing initiatives.

8 Information technology means any equipment, or interconnected system(s) or subsystem(s) of equipment, that is used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

9 Cognizant CIO means the organization's (operating unit's, bureau's, or office's) CIO.

10 The most current intake forms can be found on the SCRMP intranet page. Additional procedures, including any associated costs, may also be found on this page.

the proposal presents an acceptable risk. The cognizant CIO or designated representative may request assistance from SCRMP in making the risk determination in accordance with Enterprise Risk Management process. The cognizant CIO or designated representative and the Department's CIO shall coordinate any determinations of unacceptable risk with SCRMP and the Office of General Counsel/Contract Law Division (OGC/CLD) prior to its issuance to the contracting officer.

vi. **Determinations of Unacceptable Risk to the National Interest to the United States**
The contracting officer shall not make an award unless the cognizant CIO or designated representative has determined in writing that the proposal presents an acceptable risk and is in the interests of the United States. A proposal the cognizant CIO has determined as presenting an unacceptable risk or not in the interests of the United States will be eliminated from further consideration of award. Any debriefing involving such determination(s) will be conducted by the contracting officer and/or contract specialist, with participation by OGC/CLD and the cognizant CIO or designee and the SCRMP, as requested.

b. If the purchase request is below the micro-purchase threshold and the cognizant CIO or designated representative determines the acquisition is not subject to an SCRA, the request may be returned to and acquired by the purchase card holder as provided in the DOC Purchase Card Program (see Commerce Acquisition Manual 1313.301).

5. Supply Chain Risk Assessment Language for Solicitations and Resulting Contracts; and for Modifications of Existing Contracts.

As provided in paragraph 4(a)(i), the contracting officer shall insert the following language into solicitations and resulting contracts requiring an SCRA, and into any modifications of existing contracts.

a. **Notice of Supply Chain Risk Assessment (February 2025)**

The Department of Commerce (Department) will review the supply chain and conduct risk assessments for this acquisition. Offerors and awardees shall provide any information the Department deems necessary to facilitate its Supply Chain Risk Assessment (SCRA). By submitting its proposal, the offeror acknowledges the Department may reject any offer without recourse or explanation if the Department determines the proposal presents an unacceptable risk.

(end)

b. **Non-Destructive and Destructive Testing (February 2025)**

The Department of Commerce (Department) may engage in non-destructive and/or destructive testing of any Information Technology, equipment and software to determine whether it has the potential to negatively affect the security or performance of a Department information system.

(end)

c. **Supply Chain Risk Assessment Information (February 2025)**

The offeror/contractor shall submit the following information with its proposal or after award at the Government's request:

(A)

(1) Its identity, including that of each parent and/or subsidiary corporate entities.

(2) The identity of any proposed subcontractors (including but not limited to suppliers, distributors, and manufacturers) involved in its supply chain.

(3) The percentage any foreign ownership in or control of the entities identified under (A)(1) or (2).

(4) The means and method for physically delivering any information system, IT hardware, and/or software under the contract or task order must include the name(s) of any entity responsible for transport or storage. This information should address whether the information system, IT hardware and/or software will be direct-shipped to the Department. The means and method for virtually delivering any information system, IT hardware, and/or software under the contract or task order must include how the Department securely accesses the hardware and/or software.

(5) Whether the proposed information system, IT hardware and/or software includes a service agreement required by the contract or task order, and, if so, the identity of the contractor/subcontractor(s) who will provide this follow-on service, and how the services will be delivered/deployed (e.g., via on-site service? Remotely via internet?)

(B) Upon the Government's request, the offeror/contractor shall provide additional information if requested.

(C) The offeror/contractor shall include this language in all subcontracts (including but not limited to those with suppliers, distributors, and manufacturers) involving the development and delivery of an IT system, IT hardware and/or software under this acquisition.

(D) Supply Chain Risk Assessment Information shall be marked as contractor bid proposal information and source selection information in accordance with FAR 3.104-4 and securely transmitted to the contracting officer.

(E) By submission of its offer and/or acceptance of this contract or contract modification, the offeror/contractor represents this information is accurate and complete. Offerors and contractors shall have a continuing obligation to amend any information that changes during the evaluation period prior to award and/or during the period of performance of the contract or task order(s).

(end)

d. **Evaluation of Supply Chain Risk Assessment Information (Sept 2015)**

The Department will evaluate the information provided to assess the supply chain risk associated with the offeror's proposal and to determine if the award is in the national interest of the United States.

(end)

e. **Novation Agreement for Acquiring Certain Information Technology (February 2025)**

(1) "Novation agreement" means a legal instrument-(a) Executed by the--(i) Contractor (transferor); (ii) Successor in interest (transferee); and (iii) Government; and (b) By which, among other things, the transferor guarantees performance of the contract, the transferee assumes all obligations under the contract, and the Government recognizes the transfer of the contract and related assets. (FAR 2.101 – Definitions).

(2) The Department may in its interest recognize a successor in interest. The offeror and or subsequent awardee(s) agree as a condition of this contract, that any novation considered and recognized by the Department shall be subject to SCRA requirements, including **"Notice of**

Supply Chain Risk Assessment (February 2025)," "Non-Destructive and Destructive Testing (February 2025)," "Supply Chain Risk Assessment Information (February 2025)," and "Evaluation of Supply Chain Risk Assessment Information (Sept 2015)."

(end)

Please direct acquisition questions, such as required actions for contracting officers, to OAM_mailbox@doc.gov and information technology questions, such as those relating to the IT Checklist or the SCRA process, to DOC's SCRMP at SCRM_IOC@doc.gov.