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

PROCUREMENT MEMORANDUM 2023-12

ACTION

MEMORANDUM FOR: Senior Bureau Procurement Officials

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

OLIVIA BRADLEY
Digitally signed by OLIVIA BRADLEY
Date: 2023.09.29 08:58:13 -04'00'

André V. Mendes
Chief Information Officer

ANDRE MENDES
Digitally signed by ANDRE MENDES
Date: 2023.09.27 18:17:19 -04'00'

SUBJECT: Supply Chain Risk Assessment and Cybersecurity Requirements for Contracts

Background

Federal agencies rely extensively on information and communications technology (ICT) products and services[1] to carry out their operations. This dependence on ICT solutions has increased the complexity, diversity, and scale of the federal government's supply chain. Supply chain risk management (SCRM) is the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains.

Purpose

This procurement memorandum provides Department of Commerce-wide direction to contracting officers and purchase card holders to implement the guidance within NIST SP 800-161: "Supply Chain Risk Management Practices for Federal Information Systems and Organizations" and supply chain requirements within the Department of Commerce Enterprise Cybersecurity Policy, Section 4.1.17(IV) - System and Services Acquisition.

Required Actions

1. Program offices shall submit all new purchase requests[2] for information technology (IT), including requests below the micro-purchase threshold, to the Operating Unit (OU) Office of the Chief Information Officer (CIO) with a completed Office of Chief Information Officer's IT Compliance in Acquisition Checklist (IT Checklist) to enable the OU CIO to determine whether the acquisition is subject to supply chain risk assessment (SCRA) considerations.
2. If the OU CIO determines the acquisition is subject to a SCRA in accordance with PM 2015-08, "Supply Chain Risk Assessment Requirements for the Acquisition of Moderate-Impact and High-Impact Information Systems," the procedures of that PM apply in lieu of the following.

[1] According to the Federal Acquisition Supply Chain Security Act of 2018, ICT is information technology, information systems, and telecommunications equipment and telecommunications services.
[2] This includes purchase requests for new actions; not modifications for existing actions unless a checklist would otherwise be required.

3. If the OU CIO determines the acquisition is subject to SCRA considerations, the purchase request shall be referred to the servicing acquisition office for acquisition by a warranted contracting officer (CO), even if it otherwise might have been procured via the purchase card.
4. If the OU CIO determines the acquisition is subject to SCRA considerations, the CO shall include the subsequent language in the solicitation and resulting contract. If the acquisition is under an existing contract (e.g., an indefinite delivery, indefinite quantity contract), the CO shall modify the contract to include the subsequent language.
5. If the purchase request is below the micro-purchase threshold and the OU CIO determines the acquisition is not subject to SCRA considerations, 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).

Language for Solicitations and Resulting Contracts and for Modifications of Existing Contracts

Contracting officers shall insert the following language into solicitations and resulting contracts as indicated by the IT Checklist.

MITIGATING SUPPLY CHAIN RISK [DATE]

The Department of Commerce (DOC) utilizes a Supply Chain Risk Management (SCRM) Program to identify, assess, and monitor supply chain risks of critical vendors. The Government may use any information, public and non-public, including all-source intelligence for its analysis. The Contractor agrees that the Government may, at its own discretion, perform audits of supply chain risk processes or events consistent with other terms in the contract regarding access to records and audits. An onsite assessment may be required. Through the information obtained from a SCRM program, DOC may assess vendors and products through multiple risk lenses such as national security, cybersecurity, compliance, and finance. If supply chain risks are identified and corrective action becomes necessary, mutually agreeable corrective actions will be sought based upon specific identified risks. Failure to resolve any identified risk may result in contract termination.

(END)

Effective Date
This procurement memorandum is effective as of October 1, 2023, for all new purchase requests using the IT Compliance in Acquisition Checklist version 4.0e or later. As the implementation of the IT Compliance in Acquisition Checklist version 4.0e allows for a 30-day phase in period, if a new purchase request is submitted during this time using version 3.6, the requirements of this procurement memorandum are not required to be followed. This procurement memorandum remains in effect until rescinded.

Questions
Please direct any questions regarding this Procurement Memorandum to OAM_Mailbox@doc.gov.