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

PROCUREMENT MEMORANDUM 2015-08

SEP 30 2015

ACTION

MEMORANDUM FOR: Senior Bureau Procurement Officials

Heads of Contracting Offices

FROM: Barry E. Berkowitz **Signed**
Senior Procurement Executive and
Director for Acquisition Management

Steven I. Cooper **Signed**
Chief Information Officer

Thomas R. Predmore, Director **Signed**
Office of Security

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

1. Purpose

This Procurement Memorandum (PM) 2015-08 provides Department-wide direction to DOC Contracting Officers and Purchase Card Holders to implement the supply chain risk assessment requirements for the acquisition of new FIPS-199 moderate-impact and high-impact information systems set forth in Section 515 of the Consolidated and Further Continuing Appropriations Act, 2015, and conforms with DOC's Commerce Information Technology Requirement (CITR) CITR-0231 Pre-Acquisition Supply Chain Risk Management Assessment at https://connection.commerce.gov/sites/connection.commerce.gov/files/media/files/2015/citr-023_pre_acquisition_scr_assessment.pdf and Office of Chief Information Officer's IT Compliance in Acquisition Checklist (IT Checklist) at https://connection.commerce.gov/checklists/it-compliance-acguisition-checklist. [1]

Procurement Memorandum 2015-08 replaces Procurement Memorandum 2014-03, Supply Chain Risk Management Restrictions on Information Technology Acquisitions - Interim Guidance (Phase 1).

2. Background

IT systems rely on a global supply chain. This introduces multiple risks to federal IT systems, 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

[1] PM 2015-08 and CITR-023 do not address or alter the SCRA requirements applicable to the acquisition of any National Security System (NSS) information system, equipment, or software to be used in, on, or to support an existing or new NSS. These systems must comply with CNSSD 505 Supply Chain Risk Management (SCRM).

technical services. Section 515 of the Consolidated and Further Continuing Appropriations Act, 2015, Public Law 113-235, requires the Departments of Commerce and Justice, the National Aeronautics and Space Administration, and the National Science Foundation to conduct a supply chain risk assessment before acquiring a high-impact or moderate-impact information system.

Section 515 states:

> (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, ·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 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 Federal Bureau of Investigation and other appropriate agencies; and
> (3) in consultation with the Federal Bureau of Investigation 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.
>
> (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 and supply chain risk management experts, a mitigation strategy for any identified risks;
> (2) determined 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.

3. Supply Chain Risk Assessment

Supply Chain Risk Assessment (SCRA) is the process by which, upon request from the Operating Unit Chief Information Officer (OU CI0)[2], the Department's Office of Security (OSY) conducts a review of the proposed information system (including equipment and/or software that make up the information system) for risk of cyberespionage or sabotage and an analysis of the presumptive awardee(s) against available and relevant threat information. The OU CIO reviews

[2] The OU CIO may delegate the authority to request an SCRA. See CITR-23.

OSY's analysis and determines whether award to the presumptive awardee(s) is in the national interest of the United States.

4. Required Actions

a. Effective immediately the program office shall submit all purchase requests for information technology (IT) using funds appropriated or otherwise made available by the Consolidated and Further Continuing Appropriations Act, 2015, including requests below the micropurchase threshold, to the OU CIO with a completed IT Checklist to enable the OU CIO to determine whether the acquisition is subject to a SCRA.

b. If the OU CIO determines the acquisition is subject to a SCRA, 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.

c. If the purchase request is below the micropurchase threshold and the OU CIO determines the acquisition is not subject to a 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).

d. If the OU CIO determines the acquisition is subject to a SCRA, the CO shall include the language provided in Section 5 in the solicitation and resulting contract. If the acquisition is under an existing contract (e.g., an ID/IQ contract), the CO shall modify the contract to include the language in Section 5.

e. Upon completion of the review of initial proposals, the CO shall mark and securely transmit the SCRA information from the offerers in the competitive range or the presumptive awardee to the OU CIO and request a SCRA assessment. COs shall use the template in Attachment A. Such material shall be protected and marked as contractor bid proposal information and source selection information in accordance with FAR 3.104-4.

f. The OU CIO or designee shall check to ensure the offerer/contractor submitted the required SCRA information and transmit it and the proposal to OSY via the current DOC Secure File Transfer (SFT) solution. Any requests for additional information from the offerer/contractor shall be coordinated through the CO.

g. Using the information provided by the offerer/contractor, as well as additional analytical tools at its disposal, OSY 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. OSY's completed assessment report shall be made available to the OU CIO.

h. **OU CIO Risk Assessment Determination**

Following receipt of the completed SCRA report from OSY, the OU CIO shall assess and determine whether the proposal presents an acceptable risk. The OU CIO may request assistance from OSY in making the risk determination. The OU CIO shall coordinate any determinations of unacceptable risk with OSY and the Office of General Counsel/Contract Law Division (OGC/CLD) prior to its issuance to the CO.

i. Determinations of Unacceptable Risk to the National Interest to the United States

The CO shall not make award unless the OU CIO has determined in writing that the proposal presents an acceptable risk. A proposal determined to present an unacceptable risk will be eliminated from further consideration of award. Any debriefing involving such determination(s) will be conducted by the CO and/or contract specialist, with participation by OGC/CLD and the OU CIO or designee and OSY, as requested.

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

As provided in paragraph 4.d, COs shall insert the following language into solicitations and resulting contracts requiring a SCRA, and for modifications of existing contracts.

a. Notice of Supply Chain Risk Assessment (Sept 2015)

The Department of Commerce will review the supply chain risk and conduct a risk assessment for this acquisition. Offerers and awardees shall provide any information the Department deems necessary to facilitate its Supply Chain Risk Assessment (SCRA) including, but not limited to, the data requested by the **Supply Chain Risk Assessment Information (Sept 2015)** questionnaire included in this solicitation. By submission of its proposal, the offerer 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 (Sept 2015)

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

(end)

c. Supply Chain Risk Assessment Information (Sept 2015)

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

(4) The names and dates of birth of the offeror's/contractor's corporate officers identified under (A)(1) or (2), including this information for subcontractors (including but not limited to suppliers, distributors, and manufacturers).

(5) Whether the offerer/contractor and subcontractors (including but not limited to suppliers, distributors, and manufacturers) maintain a:

i. Formal security program that includes personnel security;
ii. Information security program;
iii. Physical security program;
iv. Cyber security program; and
v. Supply chain risk management program.

(6) The name and locations of each facility where any information system, IT hardware and/or software to be delivered under the contract or task order was designed, manufactured, packaged and stored prior to distribution.

(7) Whether a separation of duties exists during the development process of any information system, IT hardware and/or software to be delivered under the contract or task order.

(8) The means and method for delivering any information system, IT hardware and/or software to be delivered under the contract or task order, including 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.

(9) 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?)

(10) The identity of the entity that will provide disposal services of any information system, IT hardware and/or software required by the contract or task order.

(B) The Government may request and the offerer/contractor shall provide additional information if necessary.

(C) The offerer/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 offerer/contractor represents this information is accurate and complete. Offerers 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 offerer'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 (Sept 2015)

(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 offerer 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 (Sept 2015)," "Non Destructive and Destructive Testing (Sept 2015)," "Supply Chain Risk Assessment Information (Sept 2015)," and "Evaluation of Supply Chain Risk Assessment Information (Sept 2015)."**

(end)

Bureau Procurement Officials shall transmit this Procurement Memorandum immediately to their acquisition workforce, purchase card holders, and program offices.

Please direct acquisition questions, such as required actions for contracting officers, to OAM's Virna Winters at 202-482-3483 or vwinters@doc.gov and information technology questions, such as those relating to the IT Checklist or the SCRA process, to OCIO's Amy Hintz at 202-482-0542 or ahintz@doc.gov.

Attachment

Attachment A - Sample Template Requesting Risk Assessment

Memorandum Transmitting Supply Chain Risk Assessment Information and Proposal with Request for Supply Chain Risk Assessment

MEMORANDUM FOR: [Operating Unit Chief Information Officer or Designee]

FROM: [Contracting Officer (CO)]

SUBJECT: Request for Supply Chain Risk Assessment Determination under {RFP or Contract No.]

A. Enclosed for OU CIO supply chain risk assessment (SCRA) and determination of risk acceptability in accordance with Procurement Memorandum 2015-08 is the below described information from identified offerers/presumptive awardee(s) submitted in response to the subject RFP or Contract:
   - Name of Offerer/Presumptive Awardee
   - Offerer/Presumptive Awardee-Submitted SCRA Information
   - Proposal
   - Copy of previously completed OCIO IT Compliance in Acquisition Checklist {IT Checklist) indicating the acquisition is subject to SCRA.

B. This acquisition is for IT determined by the OU CIO to require SCRA (see Procurement Memorandum 2015-08)
C. Name of the IT System and Operating Unit
D. Title of RFP (or Existing Contract):
E. Brief Description of RFP or Existing Contract: [e.g., This is a NOAA acquisition for a new information system to provide for in support of NOAA's program X]
F. Priority: [High, Medium, or Normal]
G. Requested Date for Assessment/Determination (Allow a minimum of 4 weeks)
H. Planned award Date and Contract Period of Performance:
I. Program Manager Name, Title, Phone, E-mail:
J. Contracting Officer Representative Name, Title, Phone, E-mail:
K. Contract Specialist Name, Title; phone; e-mail:
L. Other Information (as/if needed)

Please provide the OU CIO supply chain risk assessment and determination of acceptable or unacceptable risk for the subject proposal by [date]. If you have any questions or require additional information, please contact me at [Name, Title, phone, e-mail.]

Enclosures

SOURCE SELECTION INFORMATION - DISTRIBUTION RESTRICTED - SEE FAR 2.101 and 3.1.04