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

PROCUREMENT MEMORANDUM 2014-03 APR 2 2 2014

ACTION

MEMORANDUM FOR: Bureau Procurement Officials for NOAA, NIST and OS

Chief Information Officers for NOAA, BIS, NIST, NTIA and OS

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

Simon Szykman
Chief Information Officer

SUBJECT: Supply Chain Risk Management Restrictions on Information Technology Acquisitions – Interim Guidance (Phase 1)

1. Purpose

This Procurement Memorandum (PM) provides interim guidance to Contracting Officers and Purchase Card Holders at National Oceanic and Atmospheric Administration (NOAA), Bureau of Industry and Security (BIS), National Telecommunications and Information Administration (NTIA), National Institute of Standards and Technology (NIST) and the Office of the Secretary (OS), until the Department of Commerce (DOC) finalizes its Supply Chain Risk Management (SCRM) process.

2. Background

Information Technology (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 technical services. Appropriation restrictions[1], referred to in this Procurement Memorandum as "Section 515", impose specific risk management requirements for four agencies, including the Department of Commerce.

Section 515 states:

> *Sec. 515.*
>
> *(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)*

[1] Previously Section 516 of the Consolidated and Further Continuing Appropriations Act, 2013 and most recently Section 515 of the Consolidated Appropriations Act, 2014

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. Implementation of Supply Chain Risk Management (SCRM) Restrictions – Phase 1

DOC is implementing SCRM restrictions in phases. Phase I is covered by this Procurement Memorandum and applies to acquisitions for:

a. Classified IT systems or IT systems that have a "High" impact FIPS-199 rating (i.e., systems that are rated high-impact from a risk perspective), as determined by the cognizant OCIO.
b. IT equipment and software, as identified by the cognizant OCIO, when used with systems identified in paragraph 3a.

4. "Covered" IT and "Cognizant" OCIOs

a. IT Systems, equipment and software included in paragraphs 3a and 3b are collectively referred to as "Covered" IT for Supply Chain Risk Management purposes.
b. The "Cognizant" OCIO is the Office of the Chief Information Officer for the affected bureau (i.e., NOAA, BIS, NTIA, and OS)

5. Affected Bureaus and Organizations in Phase 1

NOAA, BIS, NTIA, and OS have systems identified in 3a. Accordingly, Phase I applies to those organizations as well as to NIST--in NIST's role as provider of acquisition support to BIS and to NTIA. It is noted that OS also provides acquisition support to one portion of NTIA.

6. Pre-acquisition OCIO Review for all IT

All NOAA, BIS, NTIA, and OS purchase requests for IT systems, equipment and software shall be reviewed by their cognizant OCIO prior to purchase to determine if the purchase request is "covered" for SCRM purposes. The cognizant OCIO will use the IT Compliance in Acquisition Checklist (IT Checklist) at http://home.commerce.gov/cio/ITSITnew/IT_Security_Program_Documentation.html as the method to review and identify IT purchase requests as "covered" IT. The cognizant OCIO will use the IT Checklist to identify for the CO which IT systems, equipment, and software must be handled in accordance with the SCRM process, to include the determination of a need for a SCRM risk assessment and associated risk mitigation plan.

7. Information Technology Systems Not Covered under Phase 1

During Phase 1, Information Technology Systems other than those described in paragraph 3a. are not "covered" IT. However, the cognizant OCIO shall review all purchase requests for IT systems to ensure their status remains correctly identified.

8. Required Action(s)

a. Effective immediately all purchase requests, including but not limited to new task orders, for NOAA, BIS, NTIA, and OS for information technology systems, equipment, and software, including requests below the simplified acquisition and micropurchase thresholds, shall be submitted with the IT Checklist indicating whether the request includes "covered" IT.

b. If the purchase request is determined to include "covered" IT, the request shall be referred to the servicing acquisition office for acquisition by a warranted contracting officer. This includes requests which are below the simplified acquisition threshold or micropurchase thresholds and which might otherwise be acquired via the purchase card.

c. If the purchase request is determined not to include "covered" IT and is below the micropurchase threshold, the request may be returned to and acquired by the purchase card holder as provided in the DOC Purchase Card polcy. If such request is above the micropurchase threshold it shall be referred to the servicing acquisition office for acquisition by a warranted contracting officer.

d. The Contracting Officer shall include language provided in paragraph 9 in solicitations and resulting contracts for "covered" IT.

9. Language for Solicitations and Resulting Contracts

As provided in paragraph 8b, insert the following language into solicitations and resulting contracts for "covered" IT:

a. Notice of Supply Chain Risk Assessment (Interim) (Mar 2014)

Supply Chain Risk Management (SCRM) restrictions require the Department of Commerce, among others, to assess any associated risk of cyber espionage or sabotage associated with the acquisition of an information technology 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. Offerors and awardees are required to provide any information to the Department it deems necessary to facilitate its compliance with the SCRM assessment including, but not limited to, the data requested by the Supply Chain Risk Assessment Information (Mar 2014) questionnaire included in this solicitation. By submission of its proposal, the offeror acknowledges the Department retains the right to reject any offer without recourse or explanation if the Department determines the offeror

or the equipment or software offered by the offeror or awardee, presents an unacceptable risk to national security.

(end)

b. Non Destructive and Destructive Testing (Mar 2014)

The Department of Commerce may engage in non-destructive and/or destructive testing of any IT or software that it determines could negatively affect the security or performance of a Department of Commerce IT system.

(end)

c. Supply Chain Risk Assessment Information (Mar 2014)

To allow the Department of Commerce to conduct a risk assessment, the offeror shall submit the following information with its proposal:

(1) Its identity, including that of each parent and/or subsidiary corporate entities.
(2) Any proposed subcontractors involved in its supply chain.
(3) The degree of any foreign ownership in or control of the entities identified under 1 or 2.
(4) The names and dates of birth of the offeror's/contractor's corporate officers.
(5) Whether the offeror/contractor maintains a:
    (a) Formal security program that includes personnel security;
    (b) Information security program;
    (c) Physical security program;
    (d) Cyber security program; and
    (e) Supply chain risk management program.
(6) The name and locations of each facility where any IT hardware 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 IT hardware or software to be delivered under the contract or task order.
(8) The means and method for delivering any IT hardware 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 IT hardware of software will be direct-shipped to the Department.
(9) Who will provide any follow-on service required by the contract or task order.
(10) The identity of the entity that will provide disposal services of any IT hardware or software required by the contract or task order.

The Government may require additional information if necessary.

By submission of its offer and or acceptance of this contract, the offeror represents this information is accurate and complete. Offerors and awardees shall have a continuing obligation to amend any information that changes either during the source selection period or during the contract or task order performance period.

(end)

d. **Evaluation of Supply Chain Risk Assessment Information (Mar 2014)**
The Department will evaluate the information provided to assess the national security risk associated with the offeror's proposal.

(end)

e. **Novation Agreement for Acquiring Certain Information Technology (Mar 2014)**
(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 SCRM restrictions and applicable clauses, including **"Notice of Supply Chain Risk Assessment (Interim) (Mar 2014)", "Non Destructive and Destructive Testing (Mar 2014)," "Supply Chain Risk Assessment Information (Mar 2014)" and "Evaluation of Supply Chain Risk Assessment Information (Mar 2014)."**

(end)

10. OCIO Risk Assessment (Solicitations and Resulting Contracts)

a. **Transmission of Information to OCIO for Assessment of Risk**
The Contracting Officer shall provide to the cognizant OCIO the supply chain risk assessment information and other information deemed relevant (e.g., proposals) of the prospective awardee or those to be included in a competitive range of most highly rated offers. The CO shall transmit this information to the cognizant OCIO as a request for risk assessment (see 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.

b. **OCIO Assessment of Risk**
The cognizant OCIO shall assess whether the offeror or awardee and/or the equipment or software offered by offeror or awardee presents an acceptable or unacceptable risk to national security. The risk assessment includes but is not limited to the information submitted by the CO. The cognizant OCIO shall request assistance from the DOC Office of Security (OSY) as necessary. Any request for additional information or clarification from an offeror or awardee by the cognizant OCIO or OSY shall be coordinated through the CO.

c. **OCIO Risk Assessment Determination**
Based on the assessment, the cognizant OCIO shall determine whether the offeror or awardee and/or the equipment or software offered by the offeror or awardee presents an acceptable or unacceptable risk to national security. The cognizant OCIO's assessment and determination of risk acceptability should be coordinated with the OSY and OGC/CLD prior to its issuance to the CO. Offerors/Awardees and/or proposals for equipment or software offered which are determined to present an unacceptable risk to national security shall be handled in accordance with paragraph d.

d. **Determinations of Unacceptable Risk to National Security**
An offeror or awardee and/or proposed equipment or software determined by the cognizant OCIO to present an unacceptable national security risk 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 OCIO and OSY, as requested.

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

Designated Chief Information Officers shall transmit this Procurement Memorandum immediately to appropriate staff.

Please direct any acquisition questions to Virna Winters at 202-482-3483 or vwinters@doc.gov and any information technology questions to Rod Turk at 202-482-4708 or rturk@doc.gov .

Cc: T. Predmore
L. Didiuk

Attachment

Attachment A - Template

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

MEMORANDUM FOR: [Cognizant Office of Chief Information Officer (OCIO)]

FROM: [Contracting Officer (CO)]

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

A. Enclosed for OCIO's risk assessment and determination of risk acceptability per Procurement Memorandum 2014-XX is the below described information from identified offerors/awardee submitted in response to the subject RFP or Contract:
   - Name of Offeror/Contractor:
   - Entity's Supply Chain Risk Information:
   - Description of Other Information provided (e.g., proposal), as appropriate:
B. This acquisition is for ["Covered*" IT system and/or for "Covered" IT equipment and software] per PM- 2014-XX
C. Name of the "Covered" IT System and Operating Unit:
D. Title of RFP (or Existing Contract):
E. Description of RFP or Existing Contract: [E.g., This is a NOAA acquisition 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 2 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

Please provide the OCIO's supply chain risk assessment and acceptability determination of the subject offeror(s)/awardee(s) and proposed equipment or software to me by [date]. If you have any questions or require additional information, please contact me at [Name, Title, phone, e-mail.]

*Note: Per PM 2014-XX, a "Covered" IT system for SCRM purposes (Phase 1) is a classified IT system or IT system that has a "High" impact FIPS-199 rating (systems that are rated high-impact from a risk perspective), as determined by the cognizant OCIO. "Covered" IT equipment and software, is as identified by the cognizant OCIO, when used with "Covered IT Systems."

Enclosures

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