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

**PROCUREMENT MEMORANDUM 2006-06**

SEP 26 2006

**ACTION**

MEMORANDUM FOR: HEADS OF CONTRACTING OFFICES

Signed

FROM: Michael S. Sade
Director for Acquisition Management
and Procurement Executive

SUBJECT: Information Security in Acquisitions

**Background**

Information Security is an important business process that should be considered in all phases of the acquisition life cycle to ensure that data and information technology systems are adequately protected against risks of loss, misuse, and unauthorized access. In fiscal year 2005, the Department of Commerce (DOC) obligated $672 million for information technology (IT) –the largest single area of contract expenditure within the Department. Given the Department's information mission, the potential for security risks and exposure is significant. Failure to adequately address security can jeopardize mission success and undermine public confidence. Acquisition professionals provide a valuable service by bringing customers together with their Chief Information Office and Security representatives as early as possible in the acquisition process to help identify and mitigate security issues in contracts.

The Department of Commerce Office of the Inspector General (OIG) issued Inspection Reports: OSE-16513, OSE-16954, and OSE-17455 reflecting that although information security in IT service contracts is improving, a review of contracts revealed that better enforcement and oversight is needed for information security in contracts.

In response to the OIG recommendations, the Office of Acquisition Management (OAM) has been working with the Office of the Chief Information Officer (OCIO) and the Office of Security (OSY), to coordinate alignment of updated policies and procedures, and issue guidance to strengthen communication between Contracting Officials, Contracting Officer Representatives (CORs), Program Managers, and information security staff. As a result, OAM has taken the following steps to improve information security in acquisitions:

- Developing an Information Security in Acquisitions Checklist (see Attachment A) to ensure that information security is considered during requirements definition, solicitation, and award. The checklist is designed to help the Acquisition Team determine the appropriate security considerations in their contracts.

- Developing a flowchart of key information security decisions in the acquisition process (see Attachment B) that will assist Contracting professionals in determining the appropriate personnel and information technology security clauses to be incorporated, and procedures to be followed.

- Revising the Commerce Acquisition Regulation (CAR) clause 1352.239-73, *Security Requirements for Information Technology Resources* (see Attachment C), to remove outdated information and make it consistent with Federal policies and guidance.

- Revising Commerce Acquisition Manual (CAM) Chapter 1337.70, *Department of Commerce Personnel Security Processing Requirements for DOC Service Contracts* to reflect updated Office of Security (OSY) and Office of the Chief Information Officer (OCIO) policies and guidance.

- Creating the on-line course entitled "*Effectively Integrating Information Technology (IT) Security into the Acquisition Process".* This on-line course is designed to guide students through the necessary IT security considerations during each phase of the acquisition process. This course is available to all Departmental employees at no cost, at the following link: http://oamweb.osec.doc.gov/CAPPS_contracting_officer.html.

- Partnering with the OCIO to conduct Federal Information Security Management Act (FISMA) compliance reviews for IT acquisitions which allows OAM to identify areas for improvement.

**Purpose**

The purpose of this Procurement Memorandum (PM) is to provide a reference document on the importance of information security considerations in acquisitions. This PM supersedes PM 2002-01, Importance of Information Technology Security to Acquisitions, and PM 2003-09, Information Technology Security Clauses.

**Actions Required**

- Contracting professionals should work with their COR to complete the checklist for all service acquisitions. The checklist must be included as part of the overall contract file for new service acquisitions started on or after October 1, 2006.

- Contracting professionals shall insert clause 1353.237-73, *Security Requirements for Information Technology Resources* in all DOC solicitations and contracts for IT services beginning August 18, 2006.

- Contracting professionals shall insert the appropriate risk designation clause from CAM Chapter 1337.70 *Department of Commerce Security Processing Requirements for Department of Commerce Service Contracts* into all DOC solicitations and contracts for services that require contractor access to a system that processes privileged access to DOC data. In addition, Contracting professionals shall document the official contract file to include the rationale for the designated risk level.

If you have any questions regarding this memorandum, contact Virna Evans at (202) 482-3483.

Attachments

cc: Acquisition Community
Acquisition Council
Nancy DeFrancesco, OCIO
Mark Langstein, OGC
Judith Gordon, OIG

# Information Security in Acquisitions Checklist

## Background

In accordance with the Federal Information Security Management Act (FISMA), contractor access to government information or government information technology (IT) systems requires compliance with agency IT security policy. Aspects of the Department of Commerce (DOC) *IT Security Program Policy* (ITSPP) apply in many situations, such as personnel performing duties that require access to a DOC computer (from basic e-mail account on a DOC network to privileged system administrator access), to offsite services provided by a contractor for the storage or processing of DOC information on behalf of DOC.

## Instructions

This checklist shall be completed for all services acquisitions in order to determine whether the product or service to be acquired will require additional considerations for security requirements. In order to successfully complete this checklist, each question below should be addressed in coordination with all members of the Acquisition Team including: the Procurement Requestor from the program office, the Contracting Officer Representative (COR), staff from the Division/Bureau IT Security Office (ITSO), and the Contracting Official from the Division/Bureau's servicing Acquisition office.

| | | |
|---|---|---|
| 1. | Will this acquisition require services of contractor *personnel*?<br>If no, proceed to question 2.<br>If yes, proceed to question 1a. | Yes □ No □ |
| 1a | Will the personnel perform a function that requires assignment of a permanent user account for access to a system that processes privileged access (i.e., non-public) to DOC data? For example, requiring a DOC e-mail account, system administrator privileged access to a DOC system, or contractor personnel operating contractor systems that process DOC data.<br><br>If the answer to 1a above is no, then proceed to question 2.<br><br>If yes, Contracting Officials should work with the COR to:<br>i. Include the appropriate risk designation clause from Commerce Acquisition Manual (CAM), Chapter 1337.70 *Department of Commerce Security Processing Requirements for Department of Commerce Service Contracts,* into the solicitation and contract.<br>▪ Determine appropriate risk level, and assist in the coordination with DOC Office of Security (OSY) for personnel screenings, and staff from the Division/Bureau IT Security Office (ITSO) for the security plan and C&A.<br>▪ Document contract file to include the rationale for the designated risk level.<br>▪ Take appropriate action, in consultation with the COR, DOC Office of Security, and DOC Office of General Counsel, regarding any negative or questionable responses to personnel screening forms.<br><br>▪ Determine the appropriateness of allowing interim access to DOC IT systems pending favorable completion of a pre-employment check.<br>ii. Incorporate the clause *Security Requirements for Information Technology Resources (Commerce Acquisition Regulations (CAR)* 1352.239-73) (clause *73)*, into the solicitation and contract and (note* if you answer **NO** to question 3 below, include a statement in the SOW that "*The C&A requirements of clause 73 do not apply, and that a Security Accreditation Package is not required.*") The remaining requirements of clause 73 apply, and the Contracting Officials should work with the COR to ensure compliance with the DOC requirement for training of contractor personnel in IT security concepts (for more information, see DOC ITSPP section 15.3 online at http://www.osec.doc.gov/cio/ITSIT/DOC-IT-Security-Program-Policy.htm#P2282_250198). | Yes □ No □ |

| | | |
|---|---|---|
| 2. | Will this acquisition require use of a contractor-owned *IT system*, **and**<br>a. The IT system hardware components are located at an offsite contractor facility, | Yes □ No □ |
| | b. The IT system is **not** interconnected to a DOC network, | Yes □ No □ |
| | c. The contractor has exclusive administrative control to the components, ***and*** | Yes □ No □ |
| | d. The purpose of the requirement for the system is to process or store privileged access information (i.e., non-public) on behalf of the DOC? | Yes □ No □ |
| | If any of the answers to 2a-2d are no, proceed to question 3.<br>If yes, then incorporate clause 73 into the solicitation and contract and initiate certification and accreditation of the contractor system(s). Contracting Officials should work with the COR and ITSO to:<br>▪ Determine the security impact level of the IT system as High, Moderate, or Low (for more information, see DOC ITSPP section 3.4.1, online at http://www.osec.doc.gov/cio/ITSIT/DOC-IT-Security-Program-Policy.htm#P537_59784).<br>▪ Ensure Contractor understanding of the IT Security requirements for certification and accreditation (C&A) of the contractor system (for more information, see DOC ITSPP section 6.2.1 at http://www.osec.doc.gov/cio/ITSIT/DOC-IT-Security-Program-Policy.htm#P919_108188, and Appendix H at http://www.osec.doc.gov/cio/ITSIT/DOC-IT-Security-Program-Policy.htm#P4608_441377) as well as their responsibilities for participating in the development of a System Accreditation Package (SAP) (for more information, see DOC ITSPP section 6.5.2 at http://www.osec.doc.gov/cio/ITSIT/DOC-IT-Security-Program-Policy.htm#P1167_151660);<br>▪ Ensure that a federal program official is appointed to formally authorize operation of the system in accordance with DOC ITSPP section 6.2.5 (online at http://www.osec.doc.gov/cio/ITSIT/DOC-IT-Security-Program-Policy.htm#P1039_123891).<br>▪ Enforce contractor performance (timely submission of deliverables, compliance with personnel screening requirements, maintenance of secure system configurations and participation in annual IT security assessments to ensure compliance with SAP, and appropriate termination activity as appropriate). Annual assessments are required by DOC ITSPP section 5.5.2 (online at http://www.osec.doc.gov/cio/ITSIT/DOC-IT-Security-Program-Policy.htm#P855_98182). | |
| 3. | Will this acquisition require services that involve *connection* of one or more contractor-owned IT devices (such as a laptop computer or remote connection from a contractor system) to a DOC internal trusted (i.e., non-public) network, ***and*** the purpose of the requirement for the system involves processing or storage of privileged access (i.e., non-public) information on behalf of the DOC?<br>If no, proceed to question 4.<br>If yes, then incorporate the clause 73 into the solicitation and contract. Contracting Officials should work with the COR and ITSO to:<br>▪ Ensure Contractor understands and implements the IT Security requirements for system interconnections (for more information, see DOC ITSPP section 6.4 at | Yes □ No □ |

| | | |
|---|---|---|
| | http://www.osec.doc.gov/cio/ITSIT/DOC-IT-Security-Program-Policy.htm#P1141_148682), documents required Interconnection Security Agreement, and obtain written authorization from the federal official responsible for the DOC IT system to which the contractor shall connect.<br>▪ Ensure Contractor understands their possible participation in IT Security requirements for C&A of the DOC system to which they will connect (for more information, see DOC ITSPP section 6.2.1 at http://www.osec.doc.gov/cio/ITSIT/DOC-IT-Security-Program-Policy.htm#P919_108188, and Appendix H at http://www.osec.doc.gov/cio/ITSIT/DOC-IT-Security-Program-Policy.htm#P4608_441377);<br>▪ Enforce contractor performance (timely submission of deliverables, compliance with personnel screening requirements, annual assessments to ensure compliance with SAP, and appropriate termination activity as appropriate). Annual assessments are required by DOC ITSPP section 5.5.2 (online at http://www.osec.doc.gov/cio/ITSIT/DOC-IT-Security-Program-Policy.htm#P855_98182). | |
| 4. | If you answered YES to item 1a, 2, ***or*** 3, please answer the following: | |
| | a. Does your Acquisition Team include a member from your Division/Bureau IT Security Office (ITSO)? If no, explain why not and attach it to the checklist. | Yes □ No □ |
| | b. Have IT Security controls been considered for this acquisition as outlined in NIST Special Publication 800-64 (http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf)? If no, explain why not and attach it to the checklist. | Yes □ No □ |
| | c. Does the Statement of Work require offerors to meet the *DOC IT Security Program Policy & Minimum Implementation Standards* (http://www.osec.doc.gov/cio/ITSIT/DOC-IT-Security-Program-Policy.htm)? If no, explain why not and attach it to the checklist. | Yes □ No □ |
| | d. Has IT Security been considered throughout the entire procurement life cycle? (See course handbook "Effectively Integrating Information Technology (IT) Security into the Acquisition Process," Section 4 – Effective Integration: Procurement & IT System Life Cycles. A copy is available on the OAM website http://oamweb.osec.doc.gov/docs/CAPPS_IT_Security_course/handbook.pdf. If no, explain why not and attach it to the checklist. | Yes □ No □ |
| 5. | If you answered YES to item 1, ***and*** NO to items 1a, 2, ***and*** 3, have you included a statement in the SOW that "The C&A requirements of clause 73 do not apply, and that a Security Accreditation Package is not required?" | Yes □ No □ |

## Signatures

Please provide the name and telephone number of each Acquisition Team member who participated in completing this checklist. By signing this checklist, the Contracting Officer is representing that Security was considered for this requirement through coordination with members of the Acquisition Team including the program/requesting office's IT Security Office.

**Contracting Officer Representative:**

| | |
|---|---|
| **Name:** | **Phone:** |
| **Signature:** | **Date:** |

**Program/Requesting Office IT Security Officer:**

| | |
|---|---|
| **Name:** | **Phone:** |
| **Signature:** | **Date:** |

**Contracting Officer:**

| | |
|---|---|
| **Name:** | **Phone:** |
| **Signature:** | **Date:** |

**Other Team Members participating in the acquisition:**

| | |
|---|---|
| **Name:** | **Phone:** |
| **Title:** | |
| **Signature:** | **Date:** |

**Other Team Members participating in the acquisition:**

| | |
|---|---|
| **Name:** | **Phone:** |
| **Title:** | |
| **Signature:** | **Date:** |

**Glossary of Terms:**

**Contracting Officials:** Individuals with specific authority to process and recommend or specifically obligate the Government; includes Purchasing Agents, Contract Specialists and Contracting Officers (including program officials with Delegated Procurement Authority).

**Contracting Officer Representatives (COR)**: Individuals with specific authorities delegated from the Contracting Officer to oversee performance and assist with administration of contracts including: monitor and perform specific, enumerated contract management duties related to contract closeout and technical oversight during the performance period of a contract ensuring the contractor's performance meets the standards set forth in the contract, the technical requirements under the contract are met by the delivery date or within the period of performance, and at the price or within the estimated cost stipulated in the contract. A COR may be designated as a Level 1, 2 or 3 Contracting Officer Technical Representative (COTR) or as a Point of Contact/Order Contact (P/OC). All designations are considered Contracting Officer Representatives (CORs).

**Division/Bureau IT Security Program Manager/Chief and or IT Security Officer**: Responsible for developing and maintaining a bureau or organization's IT security program.

**Information Technology Resources** include, but are not limited to, hardware, application software, system software, and information (data). Information technology services include, but are not limited to, the management, operation (including input, processing, transmission, and output), maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

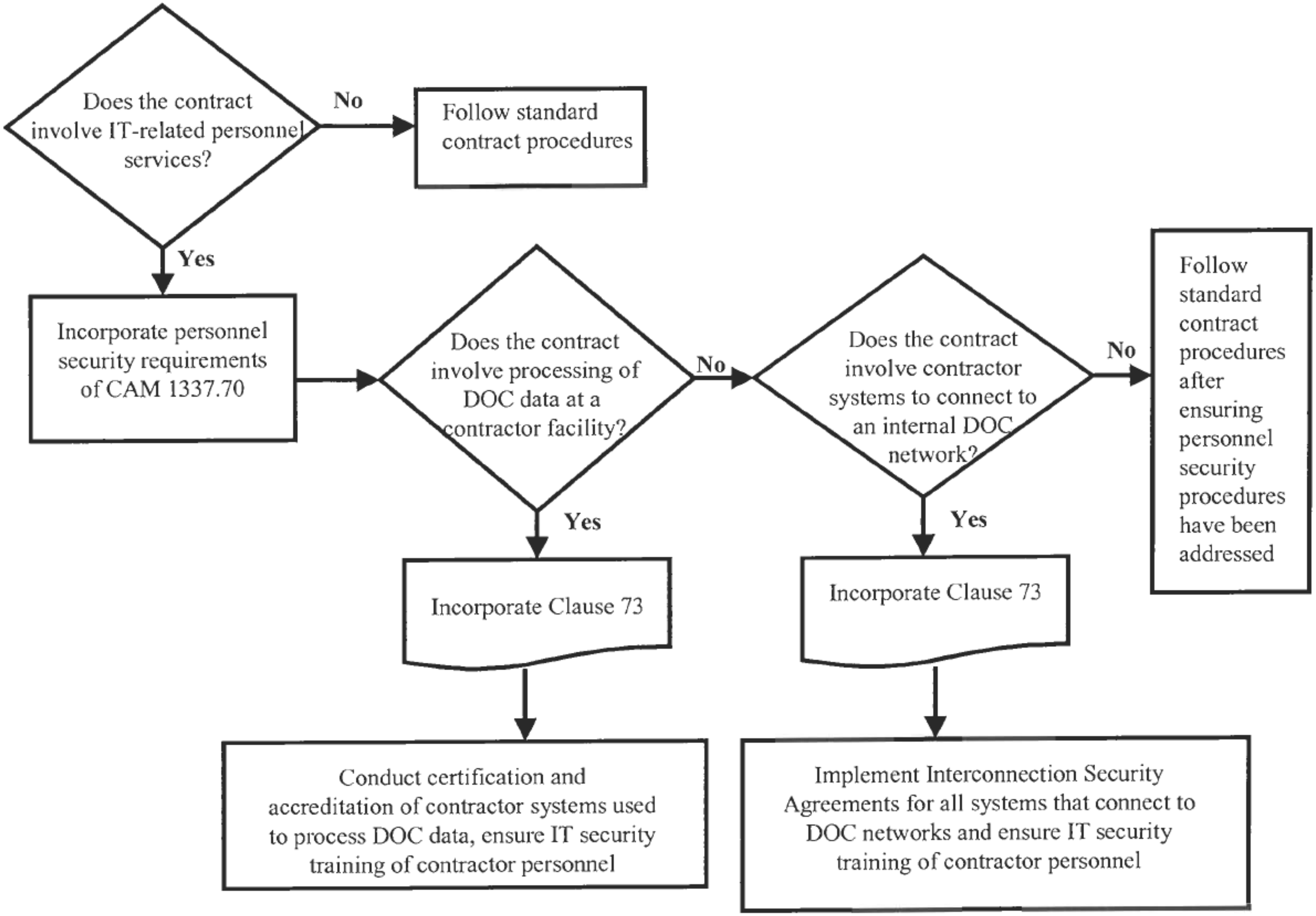
**Security Accreditation Package**: The IT security accreditation package (SAP) for a Commerce system documents the results of the security certification and provides the authorizing official with the essential information needed to make a credible, risk-based decision on whether to authorize operation of the information system. The security accreditation package contains the following documentation:

- **System Security Plan (SSP)** that has been prepared by the system owner and previously approved by the authorizing official (or their designated representative)]. The System Security Plan includes (either as supporting appendices or as references) other key security-related documents for the system including, but not limited to: the IT system security plan, risk assessment, contingency plan, incident response plan, configuration management plan, and any system interconnection agreements.

- **Security Assessment Report (SAR)** that has been prepared by the certification agent referencing the complete certification documentation package. The report_provides (i) the results of assessing the security controls in the system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the system security requirements; and (ii) recommendations for correcting deficiencies in the security controls and reducing or eliminating identified vulnerabilities.

- The supporting **Certification Documentation Package** may be maintained separately from the rest of the SAP, but must be managed by the system owner as part of the official SAP upon which the SAR was based and the accreditation decision was made.

## Flowchart of Key Information Security Decisions in the Acquisition Process


Does the contract involve IT-related personnel services?
No
Follow standard contract procedures
Yes
Incorporate personnel security requirements of CAM 1337.70
Does the contract involve processing of DOC data at a contractor facility?
No
Yes
Incorporate Clause 73
Conduct certification and accreditation of contractor systems used to process DOC data, ensure IT security training of contractor personnel
Does the contract involve contractor systems to connect to an internal DOC network?
No
Yes
Incorporate Clause 73
Implement Interconnection Security Agreements for all systems that connect to DOC networks and ensure IT security training of contractor personnel
Follow standard contract procedures after ensuring personnel security procedures have been addressed

October 2006

## CAR 1352.239-73- SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES

The Contracting Officer shall insert a clause the same as the following in all DOC solicitations and contract for Information Technology services. The following language may only be modified by adding more restrictive agency or bureau specific guidance.

## CAR 1352.239-73- SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES

(a) Applicability.

This clause is applicable to all contracts that require Contractor electronic access to Department of Commerce sensitive non-national security or national security information contained in systems, or administrative control of systems that process or store information, that directly support the mission of the Agency.

(b) Definitions.

For purposes of this clause the term "Sensitive" is defined by the guidance set forth in:

The Computer Security Act of 1987 (P.L. 100-235) (http://www.osec.doc.gov/cio/oipr/ITSec/csa-1987.html ), including the following definition of the term

(1) sensitive information "... any information, the loss, misuse, or unauthorized access, to or modification of which could adversely affect the national interest or the, conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (The Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

(2) For purposes of this clause, the term "National Security" is defined by the guidance set forth in:

- The *DOC IT Security Program Policy and Minimum Implementation Standards, Section 4.3* (http://www.osec.doc.gov/cio/ITSIT/DOC-IT-Security-Program-Policy.htm).
- The *DOC Security Manual, Chapter 18* (http://home.commerce.gov/osy/SecurityManual/Security%20Manual%20Contents2.pdf).
- Executive Order 12958, as amended, Classified National Security Information. Classified or national security information is information that has been specifically authorized to be protected from unauthorized disclosure in

the interest of national defense or foreign policy under an Executive Order or Act of Congress.

(3) Information technology resources include, but are not limited to, hardware, application software, system software, and information (data). Information technology services include, but are not limited to, the management, operation (including input, processing, transmission, and output), maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) The Contractor shall be responsible for implementing sufficient Information Technology security, to reasonably prevent the compromise of DOC IT resources for all of the contractor's systems that are interconnected with a DOC network or DOC systems that are operated by the Contractor.

(d) All Contractor personnel performing under this contract and Contractor equipment used to process or store DOC data, or to connect to DOC networks, must comply with the requirements contained in the DOC *Information Technology Management Handbook* (http://www.osec.doc.gov/cio/cio_it_policy_page.htm), or equivalent/more specific agency or bureau guidance as specified immediately hereafter [**insert agency or bureau specific guidance, if applicable**].

(e) Contractor personnel requiring a user account for access to systems operated by the Contractor for DOC or interconnected to a DOC network to perform contract services shall be screened at an appropriate level in accordance with Commerce Acquisition Manual 1337.70, *Security Processing Requirements for Service Contracts*.

(f) Within 5 days after contract award, the Contractor shall certify in writing to the COR that its employees, in performance of the contract, have completed initial IT security orientation training in DOC IT Security policies, procedures, computer ethics, and best practices, in accordance with *DOC IT Security Program Policy,* chapter 15, section 15.3. The COR will inform the Contractor of any other available DOC training resources. Annually thereafter the Contractor shall certify in writing to the COR that its employees, in performance of the contract, have completed annual refresher training as required by section 15.4 of the *DOC IT Security Program Policy*.

(g) Within 5 days of contract award, the Contractor shall provide the COR with signed acknowledgement of the provisions as contained in Commerce Acquisition Regulation (CAR), 1352.209-72, *Restrictions Against Disclosures*.

(h) The Contractor shall afford DOC, including the Office of Inspector General, access to the Contractor's and subcontractor's facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry out a program of IT inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DOC data or to the function of computer systems operated on behalf of DOC, and to preserve evidence of computer crime.

(i) For all Contractor-owned systems for which performance of the contract requires interconnection with a DOC network or that DOC data be stored or processed on them, the Contractor shall provide, implement, and maintain a System Accreditation Package in accordance with chapter 6 of the *DOC IT Security Program Policy*. Specifically, the Contractor shall:

(1) Within 14 days after contract award, the contractor shall submit for DOC approval a System Certification Work Plan, including project management information (at a minimum the tasks, resources, and milestones) for the certification effort, in accordance with *DOC IT Security Program Policy*, Section 6.5.2 and [**Insert agency or bureau specific guidance, if applicable**]. The Certification Work Plan, approved by the COR, in consultation with the DOC IT Security Officer, or Agency/Bureau IT Security Manager/Officer, shall be incorporated as part of the contract and used by the COR to monitor performance of certification activities by the contractor of the system that will process DOC data or connect to DOC networks. Failure to submit and receive approval of the Certification Work Plan may result in termination of the contract.

(2) Upon approval, the Contractor shall follow the work plan schedule to complete system certification activities in accordance with DOC IT Security Program Policy section 6.2, and provide the COR with the completed System Security Plan and Certification Documentation Package portions of the System Accreditation Package for approval and system accreditation by an appointed DOC official.

(3) Upon receipt of the Security Assessment Report and Authorizing Official's written accreditation decision from the COR, the Contractor shall maintain the approved level of system security as documented in the Security Accreditation Package, and assist the COR in annual assessments of control effectiveness in accordance with DOC *IT Security Program Policy*, section 6.3.1.2.

(j) The Contractor shall incorporate this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

**(End of clause)**