# 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,<br>b. The IT system is **not** interconnected to a DOC network,<br>c. The contractor has exclusive administrative control to the components, ***and***<br>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?<br><br>If any of the answers to 2a-2d are no, proceed to question 3.<br><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). | Yes ☐ No ☐<br>Yes ☐ No ☐<br>Yes ☐ No ☐<br>Yes ☐ No ☐ |
| 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><br>If no, proceed to question 4.<br><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 ☐ |

Requisition No. NNNN1234-12-12345, Contact: FirstName LastName - phone number

**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:** Tommy Thompson, Sr. | **Phone:** 240-678-8000 |
| **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:** |

Requisition No. NNNN1234-12-12345, Contact: FirstName LastName - phone number

**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:

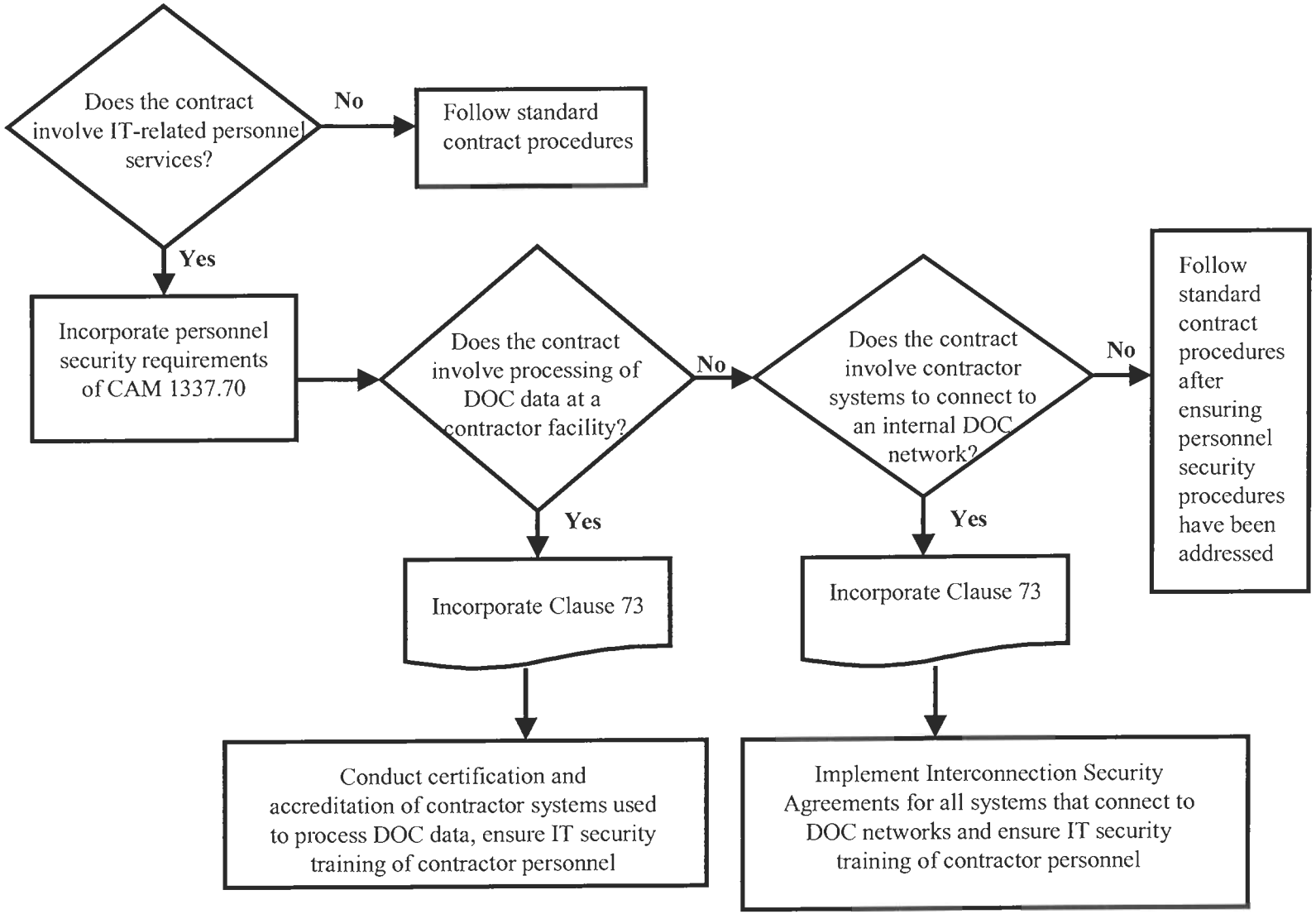
- **System Security Plan (SSP)** that has been prepared by the system owner and previously approved by the authorizing official (or their designated representative)]. The System Security Plan includes (either as supporting appendices or as references) other key security-related documents for the system 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.

Requisition No. NNNN1234-12-12345, Contact: FirstName LastName - phone number

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




Requisition No. NNNN1234-12-12345, Contact: FirstName LastName - phone number