Instructions:
This information security checklist with appropriate signatures must be completed for Information Technology (IT) acquisitions within the Department of Commerce (DOC). This represents a list of important or relevant actions (steps) that must be taken to ensure that security considerations were incorporated into IT acquisitions. You can assume that if the answer to a question does not redirect you to a new question further down the checklist, then you should proceed to the next question until you obtain the final concurrence signatures. Each checklist question should be addressed in coordination with the Acquisition team including: the Procurement Requestor from the program office, the Procurement Contracting Officer Technical Representative (COTR), OU Approved Program/ Requesting Office IT Security Officer, and Acquisition Contracting Official (CO).

Background:
Information Security is an important business process that should be considered in all phases of the acquisition process to ensure data and information technology systems are adequately protected against risk of loss, misuse, and unauthorized access. In accordance with the Federal Information Security Management Act (FISMA), contractor access to government information or government information technology (IT) systems requires compliance with the agency IT Security Policy. All information technology acquisitions must meet the requirements outlined in the Federal Acquisition Regulation (FAR) Part 39.101 (d) policy ensuring the use of common security configuration checklists in the management of risk. National Institute of Standards and Technology (NIST) defines a security configuration checklist (also called a lockdown, hardening guide, or benchmark) as a document that contains instructions for securely configuring an IT product for an operational environment or verifying that an IT product has already been securely configured. The National Checklist Program (NCP) is the U.S. government repository of publicly available security checklists that provide detailed guidance on setting the security configuration of operating systems and applications. The NCP, as defined by NIST SP 800-70 Revision 1, conforms to the Security Content Automation Protocol (SCAP) that enables numerous SCAP-validated security tools to automatically perform configuration checking using NCP checklists. Whenever feasible, organizations should apply checklists to operating systems and applications to reduce the number of vulnerabilities that attackers can attempt to exploit and to lessen the potential impact of successful attacks. *Note: The NCP checklists exclude equipment that is being acquired for specialized Research and Development (R&D) or scientific purposes.*

	System(s):	**Date:**

1	**Does this acquisition involve a hardware or software product purchase?**
	
	     Note: If the answer is No, then proceed to question 2.
	   If the answer is Yes, then include appropriate clauses into the solicitation and contract to ensure this acquisition meets DOC ITSPP media sanitization requirements, FAR 39.101(d) regulations involving NIST common security configuration checklists, including Federal Desktop Core Configuration (FDCC) or United States Government Configuration Baseline (USGCB) initiative, Homeland Security Presidential Directive 12 (HSPD-12) requirements from FAR 4.1302 stating: *(a) In order to comply with FIPS PUB 201, agencies must purchase only approved personal identity verification products and services. (b) Agencies may acquire the approved products and services from the GSA, Federal Supply Schedule 70, Special Item Number (SIN) 132-62, HSPD-12 Product and Service Components, in accordance with ordering procedures outlined in FAR Subpart 8.4.,* as well as Internet Protocol Version 6 (IPv6) requirements from FAR part 11.002 (g) stating: *Unless the agency Chief Information Officer waives the requirement, when acquiring information technology using Internet Protocol, the requirements documents must include reference to the appropriate technical capabilities defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program. The applicability of IPv6 to agency networks, infrastructure, and applications specific to individual acquisitions will be in accordance with the agency's Enterprise Architecture (see OMB Memorandum M-05-22 dated August 2, 2005).*
	
	    • . Proceed to question 2.
		Yes ☐ No ☐

2	**Will any personnel involved in this acquisition perform a function/role that requires access to a system(s) that processes non-public or sensitive DOC data?** *For example, requiring a DOC e-mail account, system administrator access to a DOC system, vendor installation/maintenance, or contractor personnel operating system(s) that process DOC data.*
	
	 Note: If the answer is No, then proceed to question 3.
	 If the answer is Yes, then Contracting Officials should work with the COTR to incorporate contract language from Commerce Acquisition Regulation (CAR) Final Rule 48 CFR 13, specifically:
	
	 • Determine and document appropriate National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems* (FIPS-PUB-199-final.pdf), Security Categorization risk designation and assist in the coordination with DOC Office of Security (OSY) for personnel screenings, and staff from the OU IT Security Office. Insert the appropriate clauses into the contract. Select from:
	   • *Security processing requirements—high or moderate risk contracts.*
	   • *Security processing requirements—low risk contracts.*
	   • *Security processing requirements—national security contracts.*
	   • *Foreign national visitor and guest access to departmental resources.*
	 • Determine and document appropriate FISMA requirements to be met in the contract, and assist in the coordination with DOC Office of Security (OSY) for personnel screenings, and the IT Security Office involving DOC ITSPP requirements for a Security Authorization (C&A).
	 • Take appropriate action, in consultation with the COTR, DOC Office of Security, and DOC Office of General Counsel, regarding the personnel screening forms.
	 • Determine the appropriateness of allowing interim access to DOC IT systems pending favorable completion of a pre-employment check.
	 • Incorporate appropriate clauses from CAR *1352.239-72 Security requirements for information technology resource* into the solicitation and contract to ensure that the requirements, such as annual IT security awareness training, are enforceable on contract personnel.
	 • Take appropriate action, in consultation with your Privacy Officer, to ensure that the services, systems, and/or products being procured comply with existing privacy laws and policies regarding protection, maintenance, dissemination and disclosure of information.
	 • In consultation with the Contracting Officer, make sure FAR and all other applicable clauses protecting personal privacy interests are included. (e.g. 48 CFR 24.104)
	 Proceed to question 3.
		Yes ☐ No ☐

3	**Will this acquisition involve Government property located at an off-site contractor-controlled facility that will be used for transmitting, processing, and storing DOC data?** If the answer is No, then proceed to question 4. If the answer is Yes, then include *CAR 1352.239-72, Security Requirements for Information Technology Resources*, into the solicitation and contract. Initiate the appropriate Security Authorization (C&A) of the contractor system(s) involved and include clauses to ensure this acquisition meets DOC ITSPP security requirements for transmitting, processing, and storing data. Proceed to question 4.	Yes ☐ No ☐

4	**Will this acquisition involve a service level agreement?**	Yes ☐ No ☐
	For example, contractor maintenance on DOC system hardware or software, Software as a Service (SaaS), i.e., Cloud Computing, or External Data Storage or Contingency Emergency Back-up facility.	
	Note: If the answer is No, then proceed to question 5.	
	• If the answer is Yes, then initiate appropriate Security Authorization (C&A) of the contractor system(s) involved and include clauses to ensure this acquisition meets DOC ITSPP security requirements for transmitting, processing, and storing data, NIST Special Publication (SP) 800-37 Revision 1: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (sp800-37-rev1-final.pdf) and SP 800-64 Revision 2, *Security Considerations in the Information System Development Life Cycle* (SP800-64-Revision2.pdf) involving nondisclosure of information. Ensure that data portability, data breach notification, and data disposal are considered in the contract. Insert clauses from Commerce Acquisition Manual (CAM) Chapter 1337.70, *Personnel Security Processing Requirements for Service Contracts (Amended)*, into the contract. Also, ensure FAR part 11.002 requirements cited on page 1, question 1 of this checklist are followed. Proceed to question 5.	
5	**Do you have any supplemental information to add to this checklist?**	Yes ☐ No ☐
	Note: If the answer is No, then proceed to *Signatures* section below to obtain signatures. If the answer is Yes, then please attach appropriate supplemental information to this checklist and proceed to *Signatures* section below to obtain signatures.	

Signatures:
By signing this checklist, the Contracting Officer is representing that operating unit information security management oversight and appropriate due diligence were considered for this acquisition process.

Procurement COR/COTR:

Name: ▨▨▨▨▨▨▨▨	**Phone:**
Signature:	
Date:	

OU approved Program/Requesting Office IT Security Officer:

Name: ▨▨▨	**Phone:**
Signature:	
Date:	

Contracting Officer:

Name: ▨▨▨	**Phone:**
Signature:	
Date:	

Information Security in Acquisition Checklist
March 2011

Question 1

Does this acquisition involve a hardware or software product purchase?

→ **No** →

Question 2

Will any personnel involved in this acquisition perform a function/role that requires access to a system(s) that processes non-public or sensitive DOC data?

→ **No** →

Question 3

Will this acquisition involve Government property located at an off-site contractor-controlled facility that will be used for transmitting, processing, and storing DOC data?

Yes ↓

DOC *ITSPP* Media Sanitization, *FAR 39.101(d) (FDCC/ USGCB),* FAR Case 2005-04, and FAR Sub Part 4.13

Yes ↓

CAR 1352.237 (70, 71, 72, or 73) And CAR 1352.239-72

No / **Yes**

Question 4

Does this acquisition involve a service level agreement?

← **No**

← CAR 1352.239-72 and DOC ITSPP

Yes ↓

DOC ITSPP, NIST SP 800-37, NIST SP 800-64, CAM Chapter 1337.70, FAR Case 2005-04, and FAR Sub Part 4.13

Question 5

Do you have any supplemental information to add to this checklist?

Yes ↓

Supplement Information

No →

Obtain Signatures

References:

Commerce Acquisition Manual Chapter 1337.70: Personnel Security Processing Requirements for DOC Service (http://oam.ocs.doc.gov/docs/CAM-1337-70-Personnel-Security-ProcessingRev061212.pdf).

Commerce Office of Security (OSY) Manual of Security Policies and Procedures: *(*http://home.commerce.gov/osy/SecurityManual/Security%20Manual%20Contents2.pdf).

Federal Acquisition Regulation (FAR) Part 39.101 (d) Policy: Use of Common Security Configurations (https://www.acquisition.gov/far/html/FARTOCP39.html references NIST website http://checklists.nist.gov).

Federal Acquisition Regulation (FAR) Subpart 4.13: Personal Identity Verification https://www.acquisition.gov/far/current/html/Subpart%204_13.html

Federal Desktop Core Configuration (FDCC): OMB M-07-18, Ensuring New Acquisitions Include Common Security Configurations, http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-18.pdf).

United States Government Configuration Baseline (USGCB): USGCB baseline initiative evolved from the Federal Desktop Core Configuration mandate (http://usgcb.nist.gov/index.html).

IT Security Program Policy: (http://home.commerce.gov/CIO/ITSITnew/DOC%20_TSPP_2009_Final_.pdf).

National Checklist Program (NCP): United States Government Repository of Publicly Available Security Checklists (http://web.nvd.nist.gov/view/ncp/repository).

NIST FIPS PUB 201-1 Change Notice 1: Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

NIST SP 800-37 Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010, (sp800-37-rev1-final.pdf).

NIST SP 800-64 Revision 2: Security Considerations in the Information System Development Life Cycle, Revision 2, October 2008, (SP800-64-Revision2.pdf).

NIST SP 800-70 Revision 1: National Checklist Program for IT Products - Guidelines for Checklist Users and Developers, September 2009, (sp800-70r1.pdf).

Security Content Automation Protocol (SCAP) Validated Products: http://nvd.nist.gov/scapproducts.cfm.

Federal Acquisition Regulation (FAR) Case 2005-041, Internet Protocol Version 6 (IPv6): http://edocket.access.gpo.gov/2009/pdf/E9-28931.pdf

Version	Date	Revised by	Comment
2	4/2009	N. Gassama/A. Helzer	Updated to include OMB 07-18 FDCC requirements
2.1	8/2009	A. Helzer (OCIO)	Updated to include OIG comments
2.2	3/2010	A. Helzer (OCIO)	Updated to include OCIO and OAM comments
2.3	6/2010	A. Helzer (OCIO)	Updated to include OU comments
2.4	8/2010	A. Helzer (OCIO)	Updated to include OGC comments
2.4.1	8/2010	A. Helzer (OCIO)	Updated to remove reference to FAR Subpart 45.5 clause
2.5	1/2011	S. Lattanze (OCIO)	Updated to include OMB IPv6 requirements: FAR Case 2005-041
2.6	3/2011	W. Graham (OCIO)	Updated to include HSPD-12 requirements: FAR Subpart 4.13

We appreciate your continued efforts to make the Department's IT security posture more effective and efficient. If you have any questions, please contact the Office of IT Security, Infrastructure, and Technology at DOCITSecurity@doc.gov.