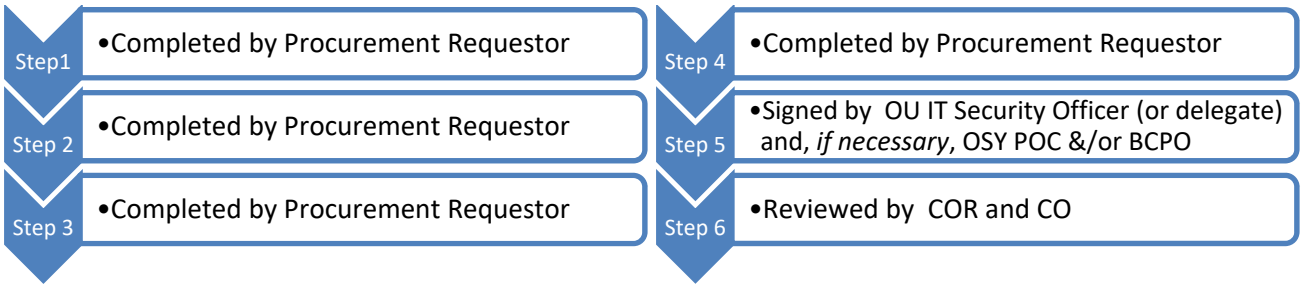
Instructions:
This IT checklist, with appropriate signatures, must be completed for Information Technology (IT) acquisitions within the Department of Commerce (DOC). It represents a list of important or relevant actions (steps) that must be taken to ensure that security considerations are incorporated into IT acquisitions. *Note: Completion of this checklist is not required for the acquisition of equipment for specialized Research and Development (R&D) or scientific purposes that are not a National Security System.*

In completing the checklist, you can assume that if the answer to a question does not redirect you to a new question further down the checklist, 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 Representative (COR), Operating Unit Approved Program/ Requesting Office IT Security Officer, and Acquisition Contracting Official (CO).



Background:
This checklist was developed to ensure that the acquisition of IT resources complies with Federal and DOC information security policy requirements and to provide a means for COs to document compliance.

	System(s): *[Provide full name of system(s) and any corresponding acronym(s)]* **Procurement Description:** *[Provide 1-2 sentences on what the IT acquisition is for]*	**Date:**
1	**Does this acquisition involve a hardware or software product purchase?** If the answer is No, proceed to question 2. If the answer is Yes, include appropriate clauses into the solicitation and contract to ensure this acquisition meets the following: • DOC IT Security Policy media sanitization requirements (MP-6) • 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 • Personal identity verification requirements from FAR 4.1302 and FIPS PUB 201 [in accordance with Homeland Security Presidential Directive (HSPD-12)] • FAR part 11.002 requirements which state that *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 (SP) 500-267)* and the corresponding declarations of conformance defined in the USGv6 Test Program. *To meet this requirement each DOC acquisition of IP protocol technology must express requirements for IPv6 capabilities in terms of the USGv6 Profile (i.e., using the USGV6 Capabilities Check List) and vendors must be required to document their product's support of the requested capabilities through the USGv6 test program (reference https://www-x.antd.nist.gov/usgv6/ using the USGv6 Suppliers Declaration of Conformity.* 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 or DOC entrusted personally identifiable information (PII) being transferred to, shared with, and/or accessed by a contractor.* If the answer is No, proceed to question 3. If the answer is Yes, Contracting Officials should work with the COR to incorporate contract language from Commerce Acquisition Regulation (CAR) Final Rule 48 CFR 13, specifically: • Determine and document contract risk using the Commerce Acquisition Manual 1337.70. Insert the appropriate clauses into the contract based on risk level. Select from the following Security Processing Requirements: • High or Moderate Risk Contracts -- 48 CFR Ch. 13 1352.237-70 • Low Risk Contracts – 48 CFR Ch. 13 1352.237.71 • National Security Contracts – 48 CFR Ch. 13 1352.237.72 • 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, see Chapter 11 Investigative Processing, of the Manual of Security Policies and Procedures, and the IT Security Office involving DOC IT Security Policy requirements for a Security Assessment & Authorization (A&A). • Take appropriate action, in consultation with the COR, OSY, 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 FAR *1352.239-72 Security Requirements for Information Technology Resources* 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. • FAR Subpart 4.19— Basic Safeguarding of Covered Contractor Information Systems o FAR Clause 52.204–21 • FAR Subpart 24.1—Protection of Individual Privacy o FAR Clause 52.224-1 “Privacy Act Notification” o FAR Clause 52.224-2 “Privacy Act” • FAR 39.101—Acquisition of Information Technology—General—Policy • FAR 39.105—Acquisition of Information Technology—General–Privacy • FAR 39.106— Acquisition of Information Technology—General–Contract Clause o FAR Clause 52.239-1 “Privacy or Security Safeguards” • FAR Subpart 27.4--Rights in Data and Copyrights • 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, proceed to question 4. If the answer is Yes, include FAR *1352.239-72, Security Requirements for Information Technology Resources*, and incorporate the applicable privacy clauses below from the FAR ,into the solicitation and contract. Initiate the appropriate Security Assessment & Authorization (A&A) of the contractor system(s) involved and include clauses to ensure this acquisition meets DOC IT Security Policy requirements for transmitting, processing, and storing data. • FAR Subpart 4.19— Basic Safeguarding of Covered Contractor Information Systems o FAR Clause 52.204–21 • FAR Subpart 24.1—Protection of Individual Privacy o FAR Clause 52.224-1 "Privacy Act Notification" o FAR Clause 52.224-2 "Privacy Act" • FAR 39.101—Acquisition of Information Technology—General—Policy • FAR 39.105—Acquisition of Information Technology—General–Privacy • FAR 39.106— Acquisition of Information Technology—General–Contract Clause o FAR Clause 52.239-1 "Privacy or Security Safeguards" • FAR Subpart 27.4--Rights in Data and Copyrights Proceed to question 4.	Yes ☐ No ☐
4	**Will this acquisition involve a service level agreement?** *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.* If the answer is No, proceed to question 5. If the answer is Yes, initiate appropriate Security Assessment and Authorization of the contractor system(s) involved and include clauses to ensure this acquisition meets DOC IT Security Policy requirements for transmitting, processing, and storing data, NIST 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 1337.70 Section 3.3 IT Service Contracts, 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.	Yes ☐ No ☐
5	**Supply Chain Risk Assessment Requirements** **Part 1 – Section 515 Supply Chain Risk Assessment (SCRA) Applicability:** **5A. Is this an acquisition of new high-impact or moderate-impact information system?** (A new high-impact or moderate-impact information system is defined as: acquisition of a new information system that is designated as FIPS 199 moderate-impact or high-impact; is subject to the reporting requirements of 44 U. S. C. Section 3505(c) FISMA Reportable System; and for which a new system inventory record will be created and entered into the CSAM in accordance with CITR-019 Risk Management Framework (RMF). Reference CITR – 023: Pre-Acquisition Supply Chain Risk Assessment Section 6.1 at https://connection.commerce.gov/policy/20140528/it-security-program-policy-commerce-information-technology-requirements-and-policy.) If the answer to 5A is Yes, a SCRA is required. If the answer to 5A is No, a SCRA is not required. **Part 2 – National Security System (NSS) SCRA Applicability:**	Yes ☐ No ☐

	5B. Is this an acquisition for a NSS (Classified or Unclassified), including IT equipment and software? **5C If the answer to 5B is Yes, is the acquisition exclusively for any of the following types of items?** - Cabling (i.e. Cat 5 or Fiber Optic) - Cable Adaptors - Power Cable - Network Server Rack - Keyboard (Wired) - Mouse (Wired) - Items with no integrated circuitry (i.e. Monitor stands) If the answer to 5C is Yes, a SCRA is not required. If the answer to 5C is No, a SCRA is required. *The OU OCIO or designee has reviewed this purchase and confirmed a SCRA is* ☐ *or is not* ☐ *applicable.* OU OCIO Point of Contact: **Name:** **Phone:** **Signature:** **Date:** **If a SCRA is required, a warranted CO shall conduct the buy, add required language in solicitation and contract documents, and transmit vendor-provided information to the OU OCIO or designee.**	Yes ☐ No ☐ Yes ☐ No ☐
6	**Do you have any supplemental information to add to this checklist?** If the answer is No, proceed to *Signatures* section below to obtain signatures. If the answer is Yes, please attach appropriate supplemental information (i.e., project org chart, previous acquisition checklist) to this checklist and proceed to *Signatures* section below to obtain signatures.	Yes ☐ No ☐

Signatures:

By signing this checklist, the Information System Security Officer, Bureau Chief Privacy Officer (if required), Procurement COR, IT Security Officer and Contracting Officer are representing that operating unit information security management oversight and appropriate due diligence were considered for this acquisition process.

Cognizant Office of Chief Information Officer Representative (OCIO) (if needed):

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

Information System Security Officer (ISSO):

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

Bureau Chief Privacy Officer (BCPO) (BCPO signature is required if the answer to question 2 and/or 3 is "Yes.")

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

Procurement COR:

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

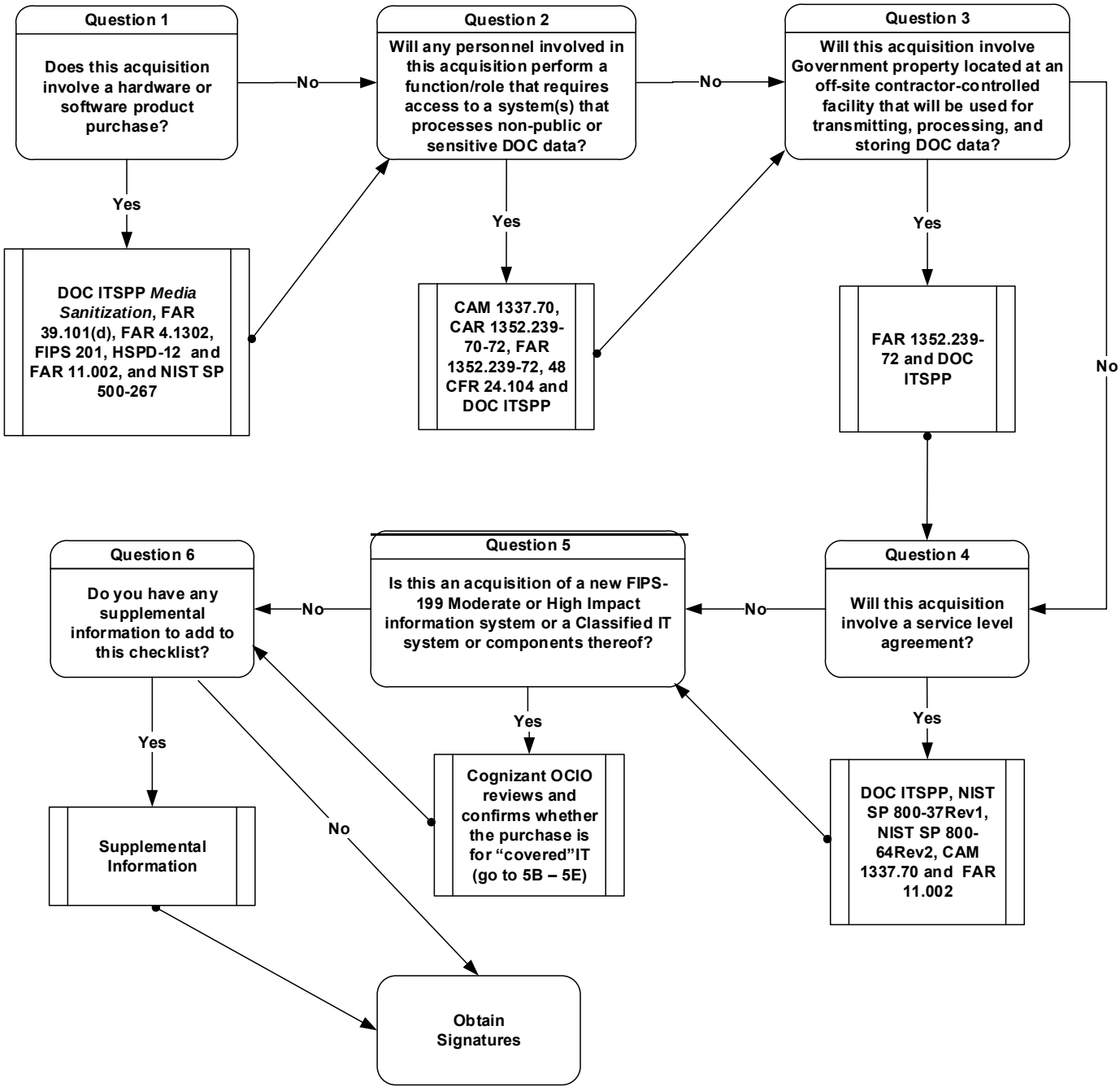
Operating Unit approved Program/Requesting Office IT Security Officer:

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

Contracting Officer:

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

IT Security Compliance in Acquisition Checklist



References:

Definition of Information Technology: includes 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. [return to instructions]

Commerce Acquisition Manual Chapter 1337.70: Personnel Security Processing Requirements for DOC Service
http://www.osec.doc.gov/oam/acquistion_management/policy/commerce_acquisition_manual_cam/documents/CAM_1337-700_Personnel_Security_Requirements.pdf

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

Commerce IT Security Policies: (https://connection.commerce.gov/policy/20140528/it-security-program-policy-commerce-information-technology-requirements-and-policy)

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

Federal Acquisition Regulation (FAR) Part 39.101 (d) Policy: Use of Common Security Configurations (https://www.acquisition.gov/sites/default/files/current/far/html/Subpart%2039_1.html#wp1096820 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 Acquisition Regulation Part 11.0002 (G) Policy: Acquiring information technology using Internet Protocol https://www.acquisition.gov/sites/default/files/current/far/html/Subpart%2011_1.html#wp1086792

Federal Desktop Core Configuration (FDCC): OMB M-07-18, Ensuring New Acquisitions Include Common Security Configurations, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-18.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 500-267: A Profile for IPv6 in the U.S. Government – Version 1.0, July 2008,
http://www.nist.gov/itl/antd/upload/usgv6-v1.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 2: National Checklist Program for IT Products - Guidelines for Checklist Users and Developers, February 2011, http://csrc.nist.gov/publications/nistpubs/800-70-rev2/SP800-70-rev2.pdf

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

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

USGv6: A Technical Infrastructure to Assist IPv6 Adoption: http://www-x.antd.nist.gov/usgv6/index.html

Version	Date	Revised by	Comment
3.6	3/16/18	P. McMahon (OCIO)	Replaced "ITSPP" with "DOC IT Security Policy" requirements. Replaced broken links: pg 1 IPV6 link, pg 6 Commerce Security Manual link & OMB M-07-18 link; Inserted privacy enhancements
3.5	7/31/15	A. Hintz (OCIO)	Updated Question 5 to reflect CITR-023: Pre-Acquisition Supply Chain Risk Assessment requirements.
3.4	4/16/14	D. Dubeau (NIST)	Replaced incorrect PM 2014-03 reference with correct reference; fixed Yes/No checkbox fields
3.3	4/16/14	H. Wald (OCIO)	Replaced PM 2014-01 under last OU ITSO signature box with PM 2014-03; corrected formatting of version table
3.2	4/15/14	P. McMahon (OCIO)	Replaced PM 2014-01 with PM 2014-03
3.1	3/14/14	P. McMahon (OCIO)	Updated Question 5 per input from OSY
3.0	2/2014	P. McMahon (OCIO)	Updated Question 5 with Section 515 legislation
2.9	11/2013	P. McMahon (OCIO)	Updated to revise SCRM content per OSY & OAM.
2.8	9/2013	P. McMahon (OCIO)	Updated to include Supply Chain Risk Management requirements and minor content changes to address Operating Unit feedback.
2.7	7/2011	P. McMahon (OCIO)	Added additional IPv6 language and reference
2.6	3/2011	W. Graham (OCIO)	Updated to include HSPD-12 requirements: FAR Subpart 4.13
2.5	1/2011	S. Lattanze (OCIO)	Updated to include OMB IPv6 requirements: FAR Case 2005-041
2.4.1	8/2010	A. Helzer (OCIO)	Updated to remove reference to FAR Subpart 45.5 clause
2.4	8/2010	A. Helzer (OCIO)	Updated to include OGC comments
2.3	6/2010	A. Helzer (OCIO)	Updated to include OU comments
2.2	3/2010	A. Helzer (OCIO)	Updated to include OCIO and OAM comments
2.1	8/2009	A. Helzer (OCIO)	Updated to include OIG comments
2	4/2009	N. Gassama/A. Helzer	Updated to include OMB 07-18 FDCC requirements