CHECKLIST FOR INFORMATION SECURITY IN THE INITIATION PHASE OF ACQUISITIONS

1. BACKGROUND

In accordance with VA policy, contractors' storage, generation, transmission or exchanging of VA sensitive information requires appropriate security controls to be in place. The VA Information Security Program policy – VA Directive and Handbook 6500 and additional 6500 series directives and handbooks - provide the framework for security within VA.

2. INSTRUCTIONS

This checklist must be completed at the **initiation** of all IT service acquisitions, statements of work, third-party service agreements and any other legally binding agreement in order to determine what, if any, security and privacy controls are necessary specifically as it relates to the VAAR security clause. OGC guidance should be sought on data ownership issues, as necessary. The checklist can also be used for other types of contracts, if appropriate or needed. In order to successfully complete this checklist, each question below must be addressed in coordination with all members of the local Acquisition Team including: the Procurement Requestor or Program Manager from the program office or facility, the Contracting Officer Representative (COR), the Information Security Officer (ISO), the Contracting Officer (CO) from the program office or facility's servicing Acquisition office, and the Privacy Officer (PO). The ISO is the arbitrator if there are questions or disagreements on the appropriate answers.

1.	Is this an acquisition or purchase of <u>only</u> commodities or goods (e.g. equipment or software)? If <u>yes</u>, then the security clause is <u>not</u> required as long as VA sensitive information is not involved. If <u>no</u>, then proceed to the next question.	Yes ☐ No ☐
2.	Does the contract involve "VA sensitive information?" (See 3. PROCEDURES a.) If <u>yes</u>, proceed to next question. If <u>no</u>, then the security clause is <u>not</u> required.	Yes ☐ No ☐
3.	Will this acquisition require services of contractor personnel? If <u>no</u>, proceed to question 5. If <u>yes</u>, proceed to next question.	Yes ☐ No ☐
4.	Will the personnel perform a function that requires access to a VA system or VA sensitive information (e.g., system administrator privileged access to a VA system, or contractor systems or processes that utilize VA sensitive information)? NOTE: See 3.a. under PROCEDURES regarding contracts and agreements concerning medical treatment for Veterans. If the answer above is <u>no</u>, then proceed to the next question. If <u>yes</u>, then VA security policies apply. Contracting Officials need to work with the Program Manager or (procurement requestor), COTR, PO, and ISO to: i. Include the appropriate risk designation of the contractors based on the PDAT determination. ii. Incorporate the security clause (Appendix B) into the contract involved and the <u>appropriate</u> security/privacy language outlined in Appendix C into the solicitation. iii. Determine if protected health information is disclosed or accessed and if a BAA is required.	Yes ☐ No ☐

5.	Will this acquisition require use of a contractor-owned Information Technology (IT) system or computer assets, **and**	Yes ☐	No ☐
	a. The IT system hardware components are located at an offsite contractor facility; **and**	Yes ☐	No ☐
	b. The IT system is **not** connected to a VA network; and	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 VA information on behalf of the VA.	Yes ☐	No ☐
	If <u>any</u> of the answers to 5a-5d are <u>no</u>, proceed to the next question. If <u>yes</u>, then VA security policies apply. Incorporate the clause from Appendix B and the appropriate security/privacy language from Appendix C respectively into the solicitation and contract and initiate planning for the certification and accreditation of the contractor system(s). Contracting Officials need to work with the COTR and ISO to: • Determine the security impact of the IT system as High, Moderate, or Low per 6500 Handbook, *Information Security Program*. • Ensure Contractor understanding of the IT security requirements for certification and accreditation (authorization) (C&A) of the contractor system. See VA Handbook 6500.3, *Certification and Accreditation*. • Ensure that the proper VA Management Official is appointed by the Certification Program Office to formally authorize operation of the system in accordance with VA Handbook 6500 and 6500.3. • Enforce contractor performance (timely submission of deliverables, compliance with personnel screening requirements, maintenance of secure system configurations and participation in annual IT Federal Information Security Management Act (FISMA) assessments to ensure compliance with FISMA		

	requirements). • Ensure yearly FISMA assessments are completed and uploaded into SMART.	
6.	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 VA internal trusted (i.e., non-public) network? If no, then include a statement in the SOW that "The C&A requirements do not apply, and that a Security Accreditation Package is not required: and proceed to the next question. If yes, then incorporate the security clause from Appendix B and the appropriate security/privacy language from Appendix C respectively into the solicitation and contract. Contracting Officials need to work with the COR and the ISO to: • Ensure contractor understands and implements the IT security requirements for system interconnection documents required per the Memorandum of Understanding or Interconnection Agreement (MOU-ISA). The standard operating procedure (SOP) and a template for a MOU-ISA are located on the Information Protection Risk Management (IPRM) Portal and can be provided to the contractor. • Ensure contractor understands their participation in IT security requirements for C&A of the VA system to which they connect. • Enforce contractor performance (timely submission of deliverables, compliance with personnel screening requirements, and appropriate termination activity as appropriate).	Yes ☐ No ☐
7.	Is the acquisition a service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a MOU-ISA for system interconnection? If no, then specify the mechanism/documentation used to ensure the VA sensitive information is protected.	Yes ☐ No ☐

	If yes, then incorporate the security clause and the appropriate security language from Appendices B and C into the solicitation and contract. The COTR needs to: • Ensure that a Contractor Security Control Assessment (CSCA) is completed within 30 days of contract approval and yearly on the renewal date of the contract. • Ensure that the CSCA is sent to the ISO and the OCS Certification Program Office for review to ensure that appropriate security controls are being implemented in service contracts. • Ensure a copy of the CSCA is maintained in the Security Management and Reporting Tool (SMART) database. COTR will provide a copy of the completed CSCA to ISO for uploading into SMART database.	

3. 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 or requesting office's IT Security point of contact.

(1) Contracting Officer Representative:

Name:	Phone:
Signature:	Date:

(2) Information Security Officer:

Name:	Phone:
Signature:	Date:

(3) Contracting Officer:

Name:	Phone:
Signature:	Date:

(4) Procurement Requestor/Program Manager:

Name:	Phone:
Title:	
Signature:	Date:

(5) Privacy Officer:

Name:	Phone:
Signature:	Date:

(6) Other Team Members participating in the acquisition (e.g., Records Management Officer/Compliance Officer):

Name:	Phone:
Title:	
Signature:	Date: