HSAM Appendix G - Checklist for Sensitive Information - U.S. Coast Guard

Procurement Title:

Requisition #:

Total Estimated Procurement Value (TEPV):
(Total contract cost including base award and all options)

Instructions: The requiring office shall complete this checklist for all acquisitions, including assisted acquisitions, regardless of dollar value. A properly executed checklist serves as the high risk determination required by HSAR Class Deviation 15-01, Safeguarding of Sensitive Information.

If the requiring official determines or is unclear if a contractor will have access to sensitive information and/or contractor IT systems will be used to input, store, process, output and/or transmit sensitive information, the requiring official shall ensure the Statement of Work (SOW), Statement of Objective (SOO), Performance Work Statement (PWS) or specification is reviewed by the organizations and obtain signatures, as applicable, on the final page of this checklist. The final page of this checklist provides routing instructions.

Reminder: Regardless of the HSAM Appendix G review outcomes, in accordance with Management Letter (21-01), Managing Contractor Proposed Cyber/IT-Related Solutions, the requiring office must include language in their requirements document SOW, PWS or SOO for the offeror or contractor to notify the Contracting Officer's Representative and Contracting Officer about any IT where the offeror or contractor may propose cyber/IT-related hardware, software, and/or services as a part of its solution to the government requirement that the CIO's office DID NOT previously approve prior to purchase, use and/or implement; the new required language is incorporated in the latest templates for the SOW, PWS, and SOO available in the Acquisition Road Map's (ARM) Document Search. When USCG offices receives these notifications, they must follow the procedures provided in the ML.

A. Sensitive Information and Access Requirements (completed by the requiring office)**:**

1. Will the contractor have access to any of the types of the sensitive information listed below during the acquisition?

☐ Yes ☐ No Chemical-terrorism Vulnerability Information (CVI)
☐ Yes ☐ No For Official Use Only (FOUO)
☐ Yes ☐ No Law Enforcement Sensitive Information
☐ Yes ☐ No Protected Critical Infrastructure Information (PCII)
☐ Yes ☐ No Personally Identifiable Information (PII)
☐ Yes ☐ No Sensitive PII (SPII)
☐ Yes ☐ No Sensitive Security Information (SSI)
☐ Other type of sensitive or classified information:

2. Will contractor employees have access to USCG information systems? ☐ Yes ☐ No

3. Will contractor employees require recurring access to Government facilities?
☐ Yes ☐ No

Note: If the answer is **"No"** to questions 1 through 3, proceed to the Signatures section of the checklist. When the answer is "No" to questions 1 through 3, the checklist shall, at a minimum, be signed by the requiring official and the HCA designee.

4. If the answer is **"Yes"** to either of questions 1 through 3 above, confirm that information security, personnel security, and/or privacy provisions have been identified for inclusion in the solicitation and resultant contract and coordinated with the following, as applicable (see HSAM 3004.470(b) for coordination requirements).

   Definitions:

   - **Information security provisions** include the development of the Requirements Traceability Matrix, identification of incident reporting and response requirements, and requests for the contractor to: provide security authorization documentation, obtain an independent assessment, perform continuous monitoring, provide the Government with necessary access to perform security reviews, comply with federal reporting requirements. *If information security provisions apply, CIO should be included in the review.*

   - **Personnel security provisions** include reviewing fitness requirements and other security matters related to access to sensitive but unclassified information and recurring access of contractor employees to Government facilities, information systems, security items or products. *If personnel security provisions apply, CSO should be included in the review.*

   - **Privacy provisions** include requirements for handling PII and/or SPII, incident reporting, notification and credit monitoring. *If privacy provisions apply, Privacy Officer should be included in the review.*

   If the answer is **"No"** for a required reviewing office, then written justification must be provided to explain why the reviewing office was excluded.

   ☐ Yes ☐ No ☐ N/A USCG Chief Information Officer (CIO) or designee
   ☐ Yes ☐ No ☐ N/A USCG Chief Security Officer (CSO) or designee
   ☐ Yes ☐ No ☐ N/A USCG Privacy Officer or designee
   ☐ Yes ☐ No ☐ N/A Transportation Security Administration (TSA) SSI Program Office
   ☐ Yes ☐ No ☐ N/A Cybersecurity & Infrastructure Security Agency (CISA) CVI Program Office
   ☐ Yes ☐ No ☐ N/A Cybersecurity && Infrastructure Security Agency (CISA) PCII Program Office

   Note: ***Each of the above offices has five (5) business days to adjudicate and sign submitted documents. Please allow sufficient time for the review based on the type of sensitive information included.***

5. Has the USCG CIO, CSO, Privacy Officer, HCA (or designee for each) and program manager determined that this effort will have a "high risk" of unauthorized access to or disclosure of sensitive information in accordance with the requirements of HSAR Deviation 15-01, Safeguarding of Sensitive Information, applicable to this acquisition?
   ☐ Yes ☐ No

   Note: If the answer to this question is "Yes" special clauses Safeguarding of Sensitive Information (MAR 2015), Information Technology Security and Privacy Training (MAR

2015) and HSAR clause 3052.204-71 Contractor Employee Access shall be included without revision in the solicitation and subsequent contract (as defined in FAR 2.101).

6. If the answer is "Yes" to any of the preceding questions, identify and describe the information security, personnel security, and privacy provisions to be included in the solicitation including the special clauses from HSAR Class Deviation 15-01, Safeguarding of Sensitive Information if applicable.

7. If foreign end products or services are allowed under the contract, what additional security provisions are to be included in the solicitation to protect sensitive information and facilities from unauthorized access and disclosure?

B. Authority to Operate (ATO) and Continuous Monitoring Data Requirements (completed by requiring office in coordination with USCG CIO or designee)**:**

1. Will contractor IT systems be used to input, store, process, output, and/or transmit sensitive information? ☐ Yes ☐ No

2. If "Yes" to #1, has the requiring office coordinated development of the Requirements Traceability Matrix (RTM) with the USCG CIO or designee for inclusion in the solicitation? ☐ Yes ☐ N/A (only if "No" to #1)

3. If "Yes" to #1, will the solicitation require the submission of a draft security plan and instructions on how the draft security plan will be evaluated? ☐ Yes ☐ N/A (only if "No" to #1)

4. If “Yes” to #1, does the requirements document identify how the contractor should submit monthly continuous monitoring data to the Government? ☐ Yes ☐ N/A (only if “No” to #1)

5. If “Yes” to #1, identify and describe the continuous monitoring data requirements to be included in the solicitation.

Note: When a contractor IT system will be used to input, store, process, output, and/or transmit sensitive information, the RTM shall be included in the solicitation. The RTM is prepared by the USCG CIO or designee in coordination with the requiring office and shall be included in the procurement request package as an attachment to the requirements document (i.e., Statement of Work, Statement of Objectives, Performance Work Statement). Contracting officers shall ensure the solicitation requires vendors to submit a draft security plan with their proposal/quotation as their response to the RTM. Instructions on how the draft security plan will be evaluated shall be included in the solicitation.

C. Data Retention Requirements (completed by requiring office)**:**

1. Will the contractor be required to retain sensitive information for the Government? ☐ Yes ☐ No

2. If “Yes” to #1, does the requirements document identify (a) retention requirements (e.g., length of time data must be retained before return and/or destruction) and (b) security requirements for the protection of retained data? ☐ Yes ☐ N/A (only if “No” to #1)

3. If “Yes” to #1, identify and describe the retention and security requirements to be included in the solicitation.

4. Does the Government have a plan to monitor and/or ensure contractor compliance with the retention and security requirements identified? ☐ Yes ☐ N/A (only if "No" to #1)

5. If "Yes" to #1, describe the Government's plan to monitor and/or ensure contractor compliance with the retention and security requirements identified in the acquisition.

D. Additional Privacy Considerations (completed by requiring office in coordination with USCG Privacy Officer or designee)**:**

1. Is contractor support needed to complete privacy compliance documentation (Privacy Threshold Analysis, Privacy Impact Assessment, and/or System of Record Notice, as appropriate)? ☐ Yes ☐ No ☐ N/A

2. If contractor support is needed to complete the privacy compliance documentation, does the requirements document identify the activities and level of contractor support needed? ☐ Yes ☐ N/A (only if "No" or "N/A" to #1)

3. If "Yes" to #1, identify and describe the activities and level of contractor support needed to complete the privacy compliance documentation.

Signature Page Note: After Requiring Official signature, submit this HSAM Appendix G AND the requirements document (description of requirements, SOW, SOO, PWS) through IT Procurement & Acquisition Support Site (ITPASS) to initiate review to these USCG Offices or designees if the checklist instructs their input: Chief Security Officer, Chief Information Officer, and/or Privacy Officer as appropriate. Email addresses are provided for questions ONLY. If signatures are required for SSI, CVI, and PCII, the Requiring Office must submit the checklists via email AFTER USCG applicable signatures are received. The Requiring Office will provide the HSAM Appendix G for HCA Designee signature to the Contracting Officer to review and coordinate.

Role and Inclusion Guidance	Name, Title, Office, Phone # ***OR*** Reason for Exclusion	Signature (Include date if not signing electronically)
Requiring Official (or official title) To be signed by Program Manager, Contracting Officer's Representative (COR) or other Program designee.	(Name) (Title) (Organization) (Phone Number)	
USCG Chief Security Officer (CSO) or designee Include when contractor employees require recurring access to DHS facilities and/ or access to sensitive or classified information. **Email for questions only:** If <$10M: HQS-SMB-ChiefSecurityOfficer-AppendixG-0-10M@uscg.mil If ≥$10M to <$50M: HQS-SMB-ChiefSecurityOfficer-APs-10M-50M@uscg.mil If ≥$50M: HQS-SMB-ChiefSecurityOfficer-APs-50andgreater@uscg.mil	(Name) (Title) USCG, DCMS-34 (Phone Number)	
USCG Chief Information Officer (CIO) or designee Include when information systems will be used to input, store, process, output, display, and/or transmit sensitive information. **Email for questions only**: HQS-DG-LST-CG-6-HSAMReview@uscg.mil	(Name) CIO designee USCG, CG-6 (Phone Number)	
USCG Privacy Officer or designee Include when the contractor will have access to Personally Identifiable Information (PII), Personal Health Information (PHI) and/or SPII. **Email for questions only:** HQS-DG-M-CG-61-PII@uscg.mil	(Name) Privacy Officer USCG, CG-6P (Phone Number)	
Sensitive Security Information (SSI) Program Office Include when contractor employees will have to access SSI. Email : SSI@HQ.DHS.gov (if applicable submit after ITPASS coordination is completed)	(Name) TSA, SSI Program Office (Phone Number)	
Chemical-terrorism Vulnerability Information (CVI) Program Office Include when contractors will have access to CVI. Email: ISCDAcquisition.hq.dhs.gov@hq.dhs.gov	(Name) CISA, CVI Program Office (Phone Number)	
Protected Critical Infrastructure Information (PCII) Program Office Include when contractors will have access to PCII. Email: PCII-Assist@hq.dhs.gov	(Name) CISA, PCII Program Office (Phone Number)	
USCG Head of Contracting Authority (HCA) Designee If <$10M, then Contracting Officer (KO) If ≥$10M to <$50M, then Chief of the Contracting Office (COCO) If ≥$50M, then Deputy Head of Contracting Authority (HCA)	(Name) (Title) (Organization) (Phone Number)	