APPENDIX G
CHECKLIST FOR SENSITIVE INFORMATION

Procurement Title: _____ **Requisition #:** _____
Estimated Contract Value (incl. 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 that 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, Statement of Objective, Performance Work Statement or specification is reviewed by the organizations identified at HSAM 3004.470(b) and obtain signatures, as applicable, on this checklist. If it is not clear to the requiring official if the contractor will have access to sensitive information and/or if contractor IT systems will be used to input, store, process, output, and/or transmit sensitive information, the requirements official shall at a minimum consult with the Component Chief Information Officer (CIO), Chief Security Officer (CSO) and Privacy Officer. The requiring office shall submit the completed checklist as part of the procurement request package in accordance with HSAM 3004.7101. Failure to submit a completed checklist will result in the return of the procurement request package. The contracting officer is responsible for routing the checklist to the Head of Contracting Activity (HCA) or designee for signature and ensuring the solicitation and resultant contract reflect the requirements contained in the checklist.

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 information _____

2. Will contractor employees have access to DHS 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 (or designee).

4. If the answer is **"Yes"** to either of questions 1 through 3 above, have information security, personnel security, and/or privacy provisions been identified 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.

   - **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.

   - **Privacy provisions** include requirements for handling PII and/or SPII, incident reporting, notification and credit monitoring.

   ☐ Yes ☐ No ☐ N/A Component CIO or designee
   ☐ Yes ☐ No ☐ N/A Component CSO or designee
   ☐ Yes ☐ No ☐ N/A Component Privacy Officer
   ☐ Yes ☐ No ☐ N/A TSA SSI Program Office
   ☐ Yes ☐ No ☐ N/A Cybersecurity and Infrastructure Security Agency (CISA) CVI Program Office
   ☐ Yes ☐ No ☐ N/A CISA PCII Program Office

   Note: For Components and offices that do not have a Component level CIO, CSO, or Privacy Officer, the requiring official shall coordinate with the DHS Headquarters CIO, CSO and Chief Privacy Officer (or designee for each). (See HSAM 3004.470(b)(7))

5. Has the Component 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 Component 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 Component 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 Component 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 Component 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.
_____
_____

Signatures:

_____
Name Date
Program Official (or official title)
(DHS Component and Organization)
(Telephone number)

_____
Name Date
Component Chief Information Officer (CIO) or designee
(DHS Component and Organization)
(Telephone number)

_____
Name Date
Component Chief Security Officer (CSO) or designee
(DHS Component and Organization)
(Telephone number)

_____
Name Date
Component Privacy Officer or designee
(DHS Component and Organization)
(Telephone number)

_____
Name Date
TSA SSI Program Office, as applicable
(Telephone number)

_____
Name Date
CISA CVI Program Office, as applicable
(Telephone number)

_____
Name Date
CISA PCII Program Office, as applicable
(Telephone number)

_____
Name Date
Head of Contracting Activity or designee
(DHS Component and Organization)
(Telephone number)