# APPENDIX G
# INDIVIDUAL OR CLASS CHECKLIST FOR CONTROLLED UNCLASSIFIED INFORMATION

## INDIVIDUAL CHECKLIST FOR CONTROLLED UNCLASSIFIED 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. 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 when the requiring official determines that (1) contractor and/or subcontractor employees require recurring access to government facilities or access to controlled unclassified information (CUI); (2) CUI will be collected or maintained on behalf of the agency; or (3) Federal information systems, which include contractor information systems operated on behalf of the agency, will be used to collect, process, store, or transmit CUI. If it is not clear to the requiring official if the contractor will have access to CUI and/or Federal information systems, which include contractor information systems operated on behalf of the agency, will be used to collect, process, store, or transmit CUI, 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. Controlled Unclassified Information and Access Requirements** (completed by the requiring office)**:**

1. Will the contractor have access to any of the types of CUI (see CUI definition in HSAR 3002.101) listed below during the acquisition?

☐ Yes ☐ No Chemical-terrorism Vulnerability Information (CVI)
☐ Yes ☐ No Homeland Security Agreement Information
☐ Yes ☐ No Homeland Security Enforcement Information
☐ Yes ☐ No Information Systems Vulnerability Information (ISVI)
☐ Yes ☐ No International Agreement Information
☐ Yes ☐ No Operations Security Information
☐ Yes ☐ No Personnel Security Information
☐ Yes ☐ No Physical Security 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 CUI _____

**Note:** If the answer is "Yes" to any of the information types listed above, the contracting officer **shall** include HSAR 3052.204-72 Safeguarding of Controlled Unclassified Information in the solicitation and resultant contract. If "Yes" is answered for PII and/or SPII, the contracting officer **shall** also include HSAR 3052.204-73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents in the solicitation and resultant contract.

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 any of questions 1 through 3, identify the information security, personnel security, and privacy clauses and provisions to be included in the solicitation and resultant contract:

☐ Yes ☐ No FAR 52.224-3 Privacy Training – Alternate I (see FAR Class Deviation 17-03, Revision 1)
☐ Yes ☐ No HSAR 3052.204-71 Contractor Employee Access
☐ Yes ☐ No HSAR 3052.204-71 Contractor Employee Access Alt I
☐ Yes ☐ No HSAR 3052.204-71 Contractor Employee Access Alt II
☐ Yes ☐ No HSAR 3052.204-72 Safeguarding of Controlled Unclassified Information
☐ Yes ☐ No HSAR 3052.204-72 Safeguarding of Controlled Unclassified Information Alt I
☐ Yes ☐ No HSAR 3052.204-73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents
☐ Yes ☐ No Special Clause Information Technology Security Awareness Training (see HSAR Class Deviation 15-01, Revision 1)
☐ Yes ☐ No Other: _____
_____
_____

5. If foreign end products or services are allowed under the contract, what additional security provisions are to be included in the solicitation to protect CUI 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 Federal information systems, which include contractor information systems operated on behalf of the agency, be used to collect, process, store, or transmit CUI ? ☐ Yes ☐ No

2. If "Yes" to #1, has the requiring office coordinated development of the Security Requirements Traceability Matrix (SRTM) 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 Federal information systems, which include contractor information systems operated on behalf of the agency, will be used to collect, process, store, or transmit CUI , the SRTM **shall** be included in the solicitation. The SRTM 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 SRTM. 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 CUI 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 privacy compliance documentation (Privacy Threshold Analysis, Privacy Impact Assessment, and/or System of Record Notice, as appropriate) required for this procurement? ☐ Yes ☐ No ☐ N/A

2. If "Yes" to #1, has any of the following privacy compliance documentation been completed?
   ☐ Yes ☐ No ☐ N/A Privacy Threshold Analysis
   ☐ Yes ☐ No ☐ N/A Privacy Impact Assessment
   ☐ Yes ☐ No ☐ N/A System of Record Notice
   ☐ Yes ☐ No ☐ N/A Other: _____

3. Is contractor support needed to complete privacy compliance documentation? ☐ Yes ☐ No ☐ N/A

4. 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 #3)

5. If "Yes" to #3, 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)

## CLASS CHECKLIST FOR CONTROLLED UNCLASSIFIED INFORMATION

**Title:** _____

**Class Description** (Note: Each class Appendix G shall describe with reasonable specificity the class to which it applies. This description shall enable any objective reviewer to clearly determine the action reviewed falls within the scope of the class Appendix G.)**:**

_____

_____

_____

**Estimated Value** (including all actions anticipated)**:** _____

**Expiration Date** (Note: The expiration date shall not exceed five years.) _____

**Instructions:** The requiring office may complete a class checklist when it is known that there will be multiple contract actions for the same or related supplies or services or other contract actions that require essentially identical justification (see HSAM 3004.470(d). 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 when the requiring official determines that (1) contractor and/or subcontractor employees will require recurring access to government facilities or access to controlled unclassified information (CUI); (2) CUI will be collected or maintained on behalf of the agency; or (3) Federal information systems, which include contractor information systems operated on behalf of the agency, will be used to collect, process, store, or transmit CUI. If it is not clear to the requiring official if the contractor will have access to CUI and/or if Federal information systems, which include contractor information systems operated on behalf of the agency, will be used to collect, process, store, or transmit CUI, 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 class checklist shall be approved at a level no lower than the Deputy Head of the Contracting Activity (HCA) or, for FLETC, the Deputy Chief of Procurement. The contracting officer is responsible for routing the checklist to the HCA or Deputy HCA/Deputy Chief of Procurement for signature and ensuring the solicitation and resultant contract reflect the requirements contained in the checklist.

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

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

   ☐ Yes ☐ No Chemical-terrorism Vulnerability Information (CVI)
   ☐ Yes ☐ No Homeland Security Agreement Information

☐ Yes ☐ No Homeland Security Enforcement Information
☐ Yes ☐ No Information Systems Vulnerability Information (ISVI)
☐ Yes ☐ No International Agreement Information
☐ Yes ☐ No Operations Security Information
☐ Yes ☐ No Personnel Security Information
☐ Yes ☐ No Physical Security 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 CUI _____

**Note:** If the answer is "Yes" to any of the information types listed above, the contracting officer **shall** include HSAR 3052.204-72 Safeguarding of Controlled Unclassified Information in the solicitation and resultant contract. If "Yes" is answered for PII and/or SPII, the contracting officer **shall** also include HSAR 3052.204-73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents in the solicitation and resultant contract.

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 any of questions 1 through 3, identify the information security, personnel security, and privacy clauses and provisions to be included in the solicitation and resultant contract:

☐ Yes ☐ No FAR 52.224-3 Privacy Training – Alternate I (see FAR Class Deviation 17-03, Revision 1)
☐ Yes ☐ No HSAR 3052.204-71 Contractor Employee Access
☐ Yes ☐ No HSAR 3052.204-71 Contractor Employee Access Alt I
☐ Yes ☐ No HSAR 3052.204-71 Contractor Employee Access Alt II
☐ Yes ☐ No HSAR 3052.204-72 Safeguarding of Controlled Unclassified Information
☐ Yes ☐ No HSAR 3052.204-72 Safeguarding of Controlled Unclassified Information Alt I
☐ Yes ☐ No HSAR 3052.204-73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents
☐ Yes ☐ No Special Clause Information Technology Security Awareness Training (see HSAR Class Deviation 15-01, Revision 1)
☐ Yes ☐ No Other: _____

_____

_____

5. If foreign end products or services are allowed under the contract, what additional security provisions are to be included in the solicitation to protect CUI 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 Federal information systems, which include contractor information systems operated on behalf of the agency, be used to collect, process, store, or transmit CUI ?
☐ Yes ☐ No

2. If "Yes" to #1, has the requiring office coordinated development of the Security Requirements Traceability Matrix (SRTM) 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 Federal information systems, which include contractor information systems operated on behalf of the agency, will be used to collect, process, store, or transmit CUI, the SRTM **shall** be included in the solicitation. The SRTM 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 SRTM. 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 CUI 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 privacy compliance documentation (Privacy Threshold Analysis, Privacy Impact Assessment, and/or System of Record Notice, as appropriate) required for this procurement? ☐ Yes ☐ No ☐ N/A

2. If "Yes" to #1, has any of the following privacy compliance documentation been completed?
☐ Yes ☐ No ☐ N/A Privacy Threshold Analysis
☐ Yes ☐ No ☐ N/A Privacy Impact Assessment
☐ Yes ☐ No ☐ N/A System of Record Notice
☐ Yes ☐ No ☐ N/A Other: _____

3. Is contractor support needed to complete privacy compliance documentation? ☐ Yes ☐ No ☐ N/A

4. 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 #3)

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

**Signatures**:

_____
Name Date
Requiring 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
(DHS Component and Organization)
(Telephone number)

_____
Name Date
CISA CVI Program Office, as applicable
(DHS Component and Organization)
(Telephone number)

_____
Name Date
CISA PCII Program Office, as applicable
(DHS Component and Organization)
(Telephone number)

_____
Name Date
Head of the Contracting Activity or Deputy HCA/Deputy Chief of Procurement
(DHS Component and Organization)
(Telephone number)