## Subchapter 3004.4 Safeguarding Classified and Controlled Unclassified Information Within Industry

### 3004.403 Responsibilities of contracting officers.

(a) *Presolicitation phase.* DHS is covered by the National Industrial Security Program (NISP) when a classified acquisition as defined under FAR 2.101 is proposed. The contracting officer in coordination with the requiring office/project manager and DHS Office of Security or the Component's cognizant Security Office are responsible for determining whether access to classified information will be required during contract performance by a contractor or any of its employees. Results of any determination must be discussed in the Acquisition Plan (see Appendix Z - DHS Acquisition Plan Template). When classified information is required by the contractor during contract performance, contracting officers shall adhere to the following rules and regulations:

(1) Executive Order 12829, National Industrial Security Program (NISP);

(2) DHS Instruction 121-01-011, Department of Homeland Security Administrative Security Program;

(3) Department of Defense (DOD) 5220.22-M, National Industrial Security Program Operating (NISPOM); and

(4) FAR Subpart 4.4.

(b) *Solicitation phase.* Contracting officers shall ensure that classified acquisitions are conducted as required by the NISP. When handling classified information, contracting officers shall also comply with DHS Instruction 121-01-011, Department of Homeland Security Administrative Security Program, and any Component implementing procedures. A DD Form 254, Contract Security Classification Specification, is required and completed if an offeror will need access to classified information to prepare their proposals. Contracting officers shall contact their cognizant DHS Security Office in accordance with DHS Instruction 121-01-011, when preparing contract security specifications and processing DD-254 requirements for contractor or facility security clearances for classified acquisitions.

Contracting officers should take note of the Information Security Oversight Officer (ISOO) Joint Notice 2024-01 entitled 'Joint Ventures and Entity Eligibility Determinations' when dealing with solicitations and awards where contractor access to classified information is required and joint ventures are, or could potentially be, involved.

(c) *Award phase*. Contracting officers shall ensure that DD Form 254, including solicitation or contract number, place of performance information, requirements, and required classified guidance, is forwarded to their cognizant Security Office prior to the release of classified information. (A DD 254 may need to be prepared and included in the contract although no DD 254 was required for the solicitation.)

(d) *Contract Administration.* The requiring office/project manager, the contracting officer, Contracting Officer's Representative (COR), security officials and the contractor are responsible

for effective contract administration to include revisions of the DD 254 due to contract modifications during performance and contract closeout. DD 254s must be updated if there are changes to contractor or subcontractor information, place of performance, or classification.

**3004.470 Security requirements for contractor access to unclassified facilities, information resources, and controlled unclassified information.**

**3004.470-3 Policy.**

(a) The following DHS publications apply to acquisitions where contractor employees require recurring access to unclassified facilities; access to information resources; or access to controlled unclassified information (CUI), including personally identifiable information (PII) and sensitive PII (SPII):

(1) DHS MD Number 140-01, Information Technology (IT) Systems Security and DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems; (2) DHS MD Number 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information;

(3) DHS MD Number 11056.1, Sensitive Security Information (SSI);

(4) DHS Directive Number 121-01, Office of the Chief Security Officer, Instruction Handbook Number 121-01-007, The DHS Personnel Security, Suitability and Fitness Program, Instruction Handbook Number 121-01-011, Department of Homeland Security Administrative Security Program;

(5) Instruction 121-01-022, Interim Procedures for Integrating the Controlled Unclassified Information Framework at the Department of Homeland Security (Note: DHS is in the process of transitioning to the CUI framework and has not yet adopted CUI markings. Homeland Security Agreement Information, Homeland Security Enforcement Information, International Agreement Information, Information Systems Vulnerability Information (ISVI), Operations Security Information, Personnel Security Information, and Physical Security Information shall be marked according to MD 11042.1 requirements for information designated as "For Official Use Only".);

(6) DHS Privacy Incident Handling Guidance; and

(7) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information.

(b) *Appendix G.* The requiring office shall complete HSAM Appendix G - Individual or Class Checklist for Controlled Unclassified Information for all acquisitions, including assisted acquisitions, regardless of dollar value. The checklist shall be coordinated with and signed by the offices listed in paragraphs (1) through (7) of this section, as applicable. The requiring office shall ensure the Statement of Work, Statement of Objectives, Performance Work Statement or specification is provided when coordinating review of the checklist. The requiring office shall submit the signed checklist to the contracting activity as part of the procurement request package.

(1) Component Chief Information Officer (CIO) or designee when information systems will be used to collect, process, store, or transmit CUI;

(2) Component Chief Security Officer (CSO) or designee when contractor employees require recurring access to DHS facilities and/or access to CUI;

(3) Component Privacy Officer or designee when the contractor will have access to PII and/or SPII;

(4) TSA Sensitive Security Information (SSI) Program Office when contractor employees will have to access SSI. As the Department-wide SSI Program Office, TSA must review all SSI requirements. The TSA SSI Program Office can be contacted at SSI@HQ.DHS.gov;

(5) Cybersecurity and Infrastructure Security Agency (CISA) Chemical-terrorism Vulnerability Information (CVI) Program Office when contractor employees will have access to CVI. As the Department-wide CVI Program Office, CISA must review all CVI requirements. The CISA CVI Program Office can be contacted at to CVI_HSAM_Requests@cisa.dhs.gov;

(6) CISA Protected Critical Infrastructure Information (PCII) Program Office when contractor employees will have access to PCII. As the Department-wide PCII Program Office, CISA must review all PCII requirements. The CISA PCII Program Office can be contacted at PCII-Assist@cisa.dhs.gov; and

(7) For Components and offices that do not have a Component level CIO, CSO, or Privacy Officer, the requirements official shall coordinate with the DHS Headquarters CIO, CSO and Chief Privacy Officer as follows:

CIO: OCIO-HSAR-Review@hq.dhs.gov
CSO: PSDContractorReview@hq.dhs.gov (classified and unclassified contracts)
Chief Privacy Officer: PrivacyContracts@hq.dhs.gov

(c) *Appendix G Exceptions and Classified Procurements.*

(1) *Foreign Military Sales.* Completion of the checklist is not required for Foreign Military Sales conducted under FAR 6.302-4 International agreement where the foreign country specifies the vendor **and** recurring access to government facilities is not required.

(2) *Classified Procurements.* The requiring office shall determine if the contractor will have access to *only* classified information or *both* CUI and classified information and complete Appendix G as follows:

(i) *Only classified information.* Completion of Appendix G is not required. Requiring offices shall follow the procedures for accessing classified information in accordance with applicable Security Classification Guides (SCG) or national security regulations.

(ii) *Both CUI and classified information.* Completion of Appendix G is required, but coordination of the Appendix G with OCSO is waived as the DD254 identifying access requirements will be processed by OCSO.

(d) If it is not clear to the requiring official if the contractor will have access to CUI, collect or maintain CUI, and/or if contractor information systems will be used to collect, process, store, or transmit CUI, the requirements official shall at a minimum consult with the Component CIO, CSO and Privacy Officer (or designee for each).

(e) The contracting officer shall route Appendix G – Individual or Class Checklist for Controlled Unclassified Information to the Head of Contracting Activity (or designee) for signature and ensure the solicitation and resultant contract reflect the requirements contained in the checklist.

(f) *Class Appendix G.* A class Appendix G may be executed using Appendix G – Class Checklist for Controlled Unclassified Information. A class may consist of contract actions for the same or related supplies or services or other contract actions that require essentially identical justification. Examples for when a class Appendix G *may* be appropriate include office supplies, such as, paper, pencils and pens or facilities maintenance, such as, janitorial services (Sensitive Compartmented Information Facility (SCIF) vs. non-SCIF). 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. For example, a description that solely states "office supplies" would be insufficient. The description would need to identify the specific type of office supplies to which the class applies.

(1) Requiring offices shall ensure each HSAM Appendix G – Class Checklist for Controlled Unclassified Information is coordinated with and reviewed by the offices identified in paragraph (b) of this section. Requiring offices shall also obtain signatures, as applicable, on the class Appendix G. If it is not clear to the requiring official if the contractor will have access to CUI, collect or maintain CUI, and/or if contractor IT systems will be used to collect, process, store, or transmit CUI, the requirements official shall at a minimum consult with the Component CIO, CSO and Privacy Officer (or designee for each).

(2) Each class Appendix G shall have an expiration date that does not exceed five years.

(3) A copy of the class Appendix G shall be placed in each individual contract file that is covered by the class determination.

(4) Contracting activities are responsible for obtaining HCA (or designee) review and approval. The class Appendix G shall be approved at a level no lower than the Deputy HCA or, for FLETC, the Deputy Chief of Procurement.

(5) The class Appendix G shall be submitted to OCPO/APL via email to Acquisition.Policy@hq.dhs.gov within 7 business days of execution.

(6) Component Acquisition Policy Offices may also submit recommendations for an enterprise level class Appendix G to Acquisition.Policy@hq.dhs.gov.

(g) *Appendix G Requirements for indefinite delivery vehicles (IDVs).* It *may* be possible to determine that all orders placed under a single or multiple award contract or agreement will result in a high risk of unauthorized access to or disclosure of sensitive information.

(1) Appendix Gs for IDVs *may* include planning for all task/delivery orders and calls to be placed against the vehicles, when feasible. The Appendix G shall specifically state that it covers all task and/or delivery orders or calls within scope of the contract or agreement. When the Appendix G includes planning for all task/delivery orders and calls to be placed against the IDV, the requiring office shall complete an Appendix G – Class Checklist for Controlled Unclassified Information. Contracting officers shall maintain a copy of the fully executed Appendix G completed for the IDV in the order file.

(2) When an Appendix G for an IDV does not cover the task/delivery orders or calls, a separate Appendix G is required for the task/delivery orders or calls. Requiring offices shall complete an Appendix G – Individual Checklist for Controlled Unclassified Information. Contracting officers shall include in the solicitation and resulting IDV, as applicable—

(i) FAR 52.224-3 Privacy Training – Alternate I (see FAR Class Deviation 17-03, Revision 1)

(ii) 3052.204-71 *Contractor Employee Access* and its Alternate I or II;

(iii) 3052.204-72 *Safeguarding of Controlled Unclassified Information* and its Alternate I;

(iv) 3052.204-73 *Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents*;

(v) Special clause Information Technology Security Awareness Training (see HSAR Class Deviation 15-01, Revision 1);

(vi) Clear instructions in the solicitation and resultant IDV on the applicability of the clauses and their Alternates; and

(vii) Ordering procedures requiring completion of an Appendix G – Individual Checklist for Controlled Unclassified Information prior to the placement of each order under the IDV.

**3004.470-70 Responsibilities.**

(a) The requiring office is responsible for determining if contractor employee access to unclassified Government facilities, information resources, or CUI will be required during contract performance. The DHS Headquarters or Component Security Offices shall assist requiring and contracting offices with identifying the risk level, suitability requirements and

other access matters relating to CUI and recurring access of contractor employees to Government facilities, information systems, security items or products (see 3004.470(b) for additional coordination requirements). All DHS OPO procurements that require contractor employees to have access to DHS facilities, CUI and/or information resources shall be coordinated with the DHS Headquarters Office of Security prior to release of the solicitation. Contracting officers and requiring officials shall coordinate the requirements for access investigations with the cognizant Component Security Office.

(b) Component Security Offices shall assist requiring offices and contracting activities by reviewing fitness requirements and other industrial or personnel security matters related to contractor employees requesting or providing support to DHS and who require unescorted access to DHS-owned facilities, DHS-controlled facilities, or commercial facilities operating on behalf of DHS; access to DHS information systems or their data; access to CUI and/or access to national security information. All Headquarters procurements meeting these requirements shall be coordinated with the DHS Office of the Chief Security Officer prior to release of the solicitation.

(c) Contracting officers and requiring officials shall coordinate the requirements for access and background investigations with the cognizant Component Security Office.

(d) Contracting officers are responsible for ensuring that solicitations, contracts, and orders identify the documentation contractor employees must complete for determining contractor suitability, especially the requirements listed in the DHS Instruction Handbook 121-01-007, Department of Homeland Security Personnel Suitability and Security Program, which is located under DHS Security and Training Requirements for Contractors, Personnel Security Policy section of the Doing Business with DHS website (https://www.dhs.gov/do-business-dhs).

(e) In order to ensure potential contractors are aware of DHS security requirements for their employees, contracting officers shall clearly identify the clearance and risk levels, as defined in the DHS Instruction Handbook 121-01-007, Department of Homeland Security Personnel Suitability and Security Program, within each solicitation. The requiring office, in conjunction with the Security Office, is responsible for providing the clearance and risk levels to contracting officers as part of its overall procurement request package.

**3004.470-71 Access to controlled unclassified information.**

(a) Contractor personnel who will require access to CUI as part of contract performance shall complete the DHS Non-disclosure Agreement (NDA), DHS Form 11000-6, before starting work under the contract. (Note: DHS is in the process of transitioning to the CUI. Homeland Security Agreement Information, Homeland Security Enforcement Information, International Agreement Information, Information Systems Vulnerability Information (ISVI), Operations Security Information, Personnel Security Information, and Physical Security Information shall be considered “Other Sensitive but Unclassified (SBU)” information when completing the form.)

(b) Contracting officers or the Component cognizant Security Office shall retain contractor signed Non-disclosure Agreements in accordance with Component procedures.