Subchapter 3004.4 Safeguarding Classified 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.

(c) *Award phase*. Contracting officers shall ensure that DD Form 254, including solicitation or contract number 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.

3004.470 Security requirements for contractor access to unclassified facilities, IT resources, and sensitive information.

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

(1) DHS MD Number 140-01, Information Technology (IT) Systems Security, the DHS Sensitive Systems Policy Directive 4300A, and the accompanying handbook, DHS 4300A Sensitive Systems Handbook;

(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) DHS Privacy Incident Handling Guidance; and

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

(b) The requiring office shall complete HSAM Appendix G - Checklist for Sensitive Information 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. 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 input, store, process, output, and/or transmit sensitive information;

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

(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 ISCDExcSec@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: DD254AdministrativeSecurity@hq.dhs.gov (classified contracts)
PSDContractorReview@hq.dhs.gov (unclassified contracts)
Chief Privacy Officer: PrivacyContracts@hq.dhs.gov

(c) If it is not clear to the requiring official if the contractor will have access to sensitive information and/or if contractor information 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 CIO, CSO and Privacy Officer.

(d) The contracting officer shall route Appendix G - Checklist for Sensitive 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.

3004.470-1 Responsibilities.

(a) The requiring office is responsible for determining if contractor employee access to unclassified Government facilities, IT resources, or sensitive but unclassified information 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 sensitive but unclassified information 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, sensitive information and/or 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 technology (IT) systems or their data; access to sensitive information 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) In addition to incorporating the clauses required by HSAR 3004.470-3 (see HSAR Class Deviation 15-01, Safeguarding of Sensitive Information), 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.

3004.470-2 Access to sensitive but unclassified information.

(a) Contractor personnel who will require access to sensitive but unclassified information as part of contract performance shall complete the DHS Non-disclosure Agreement (NDA), DHS Form 11000-6, before starting work under the contract.

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