DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

DODM5220.22V2_AFMAN16-1406V2_DAFGM2025-01

20 FEBRUARY 2025

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FLDCOMs/FOAs/DRUs

FROM: SAF/OS
1720 Air Force Pentagon
Washington, DC 20330-1665

SUBJECT: Department of the Air Force Guidance Memorandum to DoDM5220.22V2_AFMAN16-1406V2, *National Industrial Security Program: Industrial Security Procedures for Government Activities*, 8 May 2020

By Order of the Secretary of the Air Force, this Department of the Air Force Guidance Memorandum (DAFGM) immediately updates DoDM5220.22V2_AFMAN16-1406V2, *National Industrial Security Program: Industrial Security Procedures for Government Activities*. Compliance with this memorandum is mandatory. To the extent its directions are inconsistent with other Department of the Air Force publications, the information herein prevails, in accordance with Department of the Air Force Instruction (DAFI) 90-160, *Publications and Forms Management* and Department of the Air Force Manual (DAFMAN) 90-161, *Publishing Processes and Procedures*.

This guidance is applicable to the United States Space Force, Regular Air Force, the Air National Guard, the Air Force Reserve, all civilian personnel of each Air Force component, and contractor personnel performing under the terms of a properly executed classified contract with performance on an Air Force installation or within an Air Force facility, except where noted otherwise in the contract."

This DAFGM clarifies requirements for executing oversight of on-installation cleared facilities whose oversight has been formally retained by the DAF through the Installation Commander and addresses recommendations from the Air Force Audit Agency (AFAA) Cleared Facilities audit (reference Attachment 2). Updates include identifying required training for personnel performing cleared facility oversight, instituting an annual oversight reevaluation requirement, and clarifying security review oversight responsibilities.

Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction (AFI) 33-322, Records Management and Information Governance Program, and are disposed in accordance with the Air Force Records Disposition Schedule which is located in the Air Force Records Information Management System.

This Memorandum becomes void after one year has elapsed from the date of this Memorandum, or upon incorporation by interim change to, or rewrite of DODM5220.22V2_AFMAN16-1406V2, whichever is earlier.

EDWIN H. OSHIBA, SES, DAF
Director, Competitive Activities

Attachments:

1. Guidance to DoDM5220.22V2_AFMAN16-1406V2, National Industrial Security Program: Industrial Security Procedures for Government Activities
2. Report of Audit F2023-0010-A00900, *Cleared Facilities*

Attachment 1

2.7.c.(1). (**NEW**) (Added)(DAF) Individuals performing oversight of cleared facilities in support of servicing information protection office, cybersecurity, and counterintelligence oversight activities on DAF installations will, at a minimum, complete the "FSO Program Management for Possessing Facilities" and "Basic Industrial Security for the Government Security Specialist Program" (or successor) e-learning curricula on www.cdse.edu. This training will be completed within 6 months of appointment to a position providing oversight of cleared facilities, and biennially thereafter for the entirety of the individual's oversight responsibilities. The training requirement applies to personnel already executing oversight responsibilities and must be completed within 6 months from the effective date of this publication if assigned personnel with such responsibilities have not completed the training curriculum(s) within the last 2 years

2.7.c.(2). (**NEW**) (Added)(DAF) SAF/OCS or the Installation Commander, or designee, may levy additional training requirements on individuals providing oversight of cleared facilities on DAF installations, depending on the size, scope, and complexity of the oversight.

2.8.e.(5). (**UPDATED**) (Added)(DAF) When designating an on-installation contractor operation as a cleared facility and retaining oversight of the cleared facility's security program, ensure sufficient resources are allocated to include industrial security, cybersecurity, and counterintelligence support in accordance with this volume. (T-0) Sufficient resources is defined as adequately trained security specialists; counterintelligence support from the local AFOSI detachment; and cybersecurity professionals who will have the responsibility of authorizing and providing continuous monitoring of all contractor-owned and contractor-operated classified information systems resident within the on-installation cleared contractor facility. (T-1)

2.8.f. (Added) (DAF) Chief, Information Protection. The Chief, Information Protection should establish rapport with program or project managers, commanders/directors (hereinafter referred to as program/project managers), and the Director of Contracting for serviced organizations to ensure effective management of the industrial security program. The Chief, Information Protection will:

(1). (**UPDATED**) (Added)(DAF) Serve as the authority to perform industrial security program oversight for contractor operations on the installation and coordinate with DCSA when unique or special operational circumstances warrant and in all cases when the DAF provides oversight of on-installation cleared facilities. (T-1) Until an automated solution is available, Information Protection Offices (IPOs) responsible for the oversight of on-installation cleared facilities will provide copies of the completed security review reports to DCSA via encrypted email at dcsa.quantico.dcsa.mbx.ctpoperations@mail.mil (or successor email) and copy additional personnel as directed. If unable to encrypt messages, IPOs may leverage DoD SAFE to transmit to DCSA. Servicing IPO personnel will validate that the on-installation cleared facility submitted changed conditions through NISS through the facility security officer and document all changes for annotation in the SAF/OCS designated repository. (T-1)

(6). When the Installation Commander has elected to retain security cognizance of on-installation cleared facilities, accomplish the following actions:

(c). (**UPDATED**) (Added)(DAF) Receive and evaluate security violation notifications from on-installation cleared facilities. (T-1) Make notifications in accordance with this volume. (T-1) Servicing IPOs and communication squadron personnel responsible for providing oversight for on-installation cleared facilities will follow guidance in all paragraphs and subparagraphs of section 8 in this volume. (T-1)

(d). (**UPDATED**) (Added)(DAF) Maintain and make notifications regarding on-installation FCL related documentation in accordance with this volume. (T-1) Maintain up-to-date information regarding cleared facility profiles and security reviews in the SAF/OCS designated repository. (T-1) Until an automated solution is available, IPOs responsible for the oversight of on-installation cleared facilities will provide copies of the completed security review reports to DCSA via encrypted email at dcsa.quantico.dcsa.mbx.ctpoperations@mail.mil (or successor email) and copy additional personnel as directed. Servicing IPO personnel will validate that the on-installation cleared facility submitted changed conditions through NISS through the facility security officer and document all changes for annotation in the SAF/OCS designated repository. (T-1)

(e). (**NEW**) (Added)(DAF) Serve as the approving entity for all open storage areas at the on-installation cleared facility location.

(f). (**NEW**) (Added)(DAF) Conduct annual security reviews of all on-installation cleared facilities. Annual security reviews are defined as one review per calendar year. Security reviews will be conducted in accordance with section 14 of this volume.

(g) (**NEW**) (Added)(DAF) If a National Interest Determination (NID) is required, inquire about any outstanding NID requests and report back to DCSA.

2.8.i. (**NEW**) (Added)(DAF) Communication Squadron. Communication squadrons will:

(1). Review all instances of on-installation cleared facility security violations involving data spills and approve the contractor clean up procedures, in writing, or direct the contractor to receive sanitization approval from the GCA in accordance with section 8 of this volume.

(2). Ensure all classified information systems and/or classified networks installed within an on-installation cleared facility are authorized and documented in accordance with DAF guidance.

2.8.j. (**NEW**) (Added)(DAF) Air Force Office of Special Investigation (AFOSI). Supporting AFOSI detachments will:

(1). Review all instances of on-installation cleared facility security violations for counterintelligence implications and take additional actions, as applicable.
(2). Provide counterintelligence support including, but not limited to foreign travel briefings and applicable outreach events.

(3). Communicate all instances of suspicious activity to DCSA and agencies, as appropriate.

3.8.c.(4) (**UPDATED**) (Added)(DAF) SAF/OCS, serving as the designated industrial security point of contact for the DAF, will obtain this list from DCSA and share the list of all on-base cleared facilities with Installation Commanders through information protection channels to validate the information contained therein. (T-1)

3.8.c.(5). (**UPDATED**) (Added)(DAF) Installation Commanders will provide a copy of the request to DCSA to retain security cognizance of the cleared facility through Major Command/Field Command (MAJCOM/FLDCOM information protection channels to SAF/OCS. (T-1) Coordination with SAF/OCS prior to signing and submitting the request to DCSA is recommended to ensure the request is thorough and complete. In addition to including the compelling reasons to retain security cognizance, Installation Commanders will include a statement expressing commitment to sufficiently resource the oversight responsibilities. (T-1) Prior to accepting oversight responsibility for an on-installation cleared facility, the Installation Commander must coordinate with SAF/CN and host cybersecurity office to ensure cybersecurity resources are available to provide information system support and oversight for classified information system requirements, and with the SAF/IGX to ensure AFOSI resources are available to support the counterintelligence oversight requirements of this volume. (T-1)

(a) If the Commander retains security cognizance, the Commander will:

2. (**UPDATED**) (Added)(DAF) Provide sufficient security oversight support to ensure the contractor executes its industrial security responsibilities. Security Specialists designated to conduct oversight of on-installation cleared facilities must have knowledge of and be trained to the requirements of 32 CFR Part 117 (NISPOM) policy and procedures in accordance with the training requirements annotated in this DAFGM. (T-1)

4. (**UPDATED**) (Added)(DAF) IPOs will review and approve safeguarding capability for on-installation cleared facilities in accordance with the safeguarding requirements identified in 32 CFR Part 117. (T-1)

7. (**UPDATED**) (Added)(DAF) Provide a copy of the annual certification to SAF/OCS through MAJCOM/FLDCOM information protection channels. (T-1) Annual certification will:

(a). (**NEW**) (Added)(DAF) Be submitted by 31 December, or the business day immediately before 31 December, of each calendar year. (T-0). If the annual certification is delegated, the designee will provide a copy of the annual certification to the Installation Commander. (T-2).

(b). (**NEW**) (Added)(DAF) Certify that the on-installation cleared facility profile in NISS is current (T-0). The Commander will request the facility security officer provide validation, in writing, that the NISS profile is accurate and/or annotate any changes made during the calendar year with required key management personnel.

9. (**NEW**) (Added)(DAF) Installation Commanders will annually review the decision to retain security oversight of the cleared facility. This action may be completed during the annual certification process, and includes evaluating whether the information protection office, supporting communication squadron, and supporting AFOSI detachment are resourced and equipped to continue oversight activities outlined in Paragraph 3.8. of this volume, based on the size, complexity, and mission of cleared facility. (T-1)

a. (**NEW**) (Added)(DAF) This review will include an evaluation of the following criteria (at a minimum):

(1). (**NEW**) (Added)(DAF) Number of cleared contractor personnel by personnel clearance level, including cleared consultants, limited access authorizations, and employees assigned oversees.

(2). (**NEW**) (Added)(DAF) Safeguarding capabilities and complexity, including number of approved security containers, number of approved open storage areas, amount and type of classified material and hardware, presence of protected distribution system (PDS), special considerations such as COMSEC or NATO.

(3). (**NEW**) (Added)(DAF) Classified information system capabilities and complexity, including number of authorized information systems, type of authorized information systems (e.g. MUSA, WAN, federal information system, etc.), type of information systems connections.

(4). (**NEW**) (Added)(DAF) Classified visits/meetings hosted at facility.

(5). (**NEW**) (Added)(DAF) Contract and program information, including number and classification of contracts, programs, and customers the programs and customers the facility supports, type of technology involved, and subcontracts awarded.

b. (**NEW**) (Added)(DAF) The oversight will be reviewed in collaboration with information protection personnel, and the supporting communication squadron and AFOSI detachment, and relevant GCAs. Directors, Chiefs, or equivalents of supporting information protection, communications squadron, and AFOSI detachment will certify in writing that the entity is properly resourced to provide adequate cleared facility oversight support. If adequate cleared facility oversight support cannot be provided, the Director, Chief, or equivalent will ensure they immediately communicates its position to the Installation Commander.

c. (**NEW**) (Added)(DAF) If the Commander reaffirms the oversight, it will be documented through MAJCOM/FLDCOM information protection channels in the SAF/OCS designated repository. (T-1)

d. (**NEW**) (Added)(DAF) If the Commander determines conditions have changed such that a request to transfer oversight responsibility to DCSA is considered, a request will be made to DCSA to transfer security oversight responsibilities to DCSA. (T-0) Commanders will submit these requests, which must include specific rationale for transfer of oversight (i.e., what has changed to consider transfer) and address potential positive/negative mission impacts of the transfer, through MAJCOM/FLDCOM information protection channels, and will be documented in the SAF/OCS designated repository. (T-1)

8.3.a. (**UPDATED**) (Added)(DAF) When the Installation Commander provides oversight of an on-installation cleared facility, the IPO, cybersecurity squadron, and supporting AFOSI detachment will conduct the actions required of DCSA in Paragraphs 8.3.a. through 8.3.i. except where identified otherwise. (T-1) Information collected and transmitted in support of the actions set forth through paragraphs 8.3.a through 8.3.i. will be conducted through means authorized for the sensitivity and classification of the information involved (e.g. NIPRNET, SIPRNET).

b. Upon receipt of a preliminary report involving loss, compromise, or suspected compromise of classified information, DSS will:

(1) (**NEW**) (Added)(DAF) Servicing IPO personnel responsible for on-installation cleared facilities will provide an initial notification to all impacted government customers and copy SAF/OCS and/or others as directed, upon preliminary notification by the on-installation cleared facility no later than 2 duty days from contractor notification, unless otherwise documented. (T-0). Servicing IPO personnel are to retrieve GCA information from the on-installation cleared facility (e.g. government Contracting Officer). If the security violation involves another cleared defense contractor, the cognizant DCSA Field Office will be notified. The security violation case number will be documented in the following format: CAGE-YEARMODAY-C1/D1/G1. The CAGE is the CAGE code of the on-installation cleared facility. The YEARMODAY identifier is the date the violation was reported to the servicing IPO. The "C" will be used when it is a contractor reported violation. The "D" will be used if servicing IPO personnel discovered the violation. The "G" will be used if the government customer discovered the violation. The number at the end of the security violation case number format is used to document instances of a violation if the date and CAGE code are the same. For example, if the on-installation cleared facility reports two separate security violations on the same day, the security violation case number format will be numbered as "1" and "2," respectively. Initial notification to all applicable government customers can be made via email and is to include, as known, the security violation case number, impacted prime contract number, level of information involved, impacted security classification guide(s), and a preliminary summary of the violation.

(2) (**NEW**) (Added)(DAF) Servicing IPO personnel responsible for on-installation cleared facilities will provide the contractor a deadline of 20 duty days to submit the final report and will authorize extensions for the contractor as needed. (T-0)

(3) (**NEW**) (Added)(DAF) Spillage also applies to when the on-installation cleared facility is the recipient of a data spill and/or if on-site contractor or government personnel inadvertently incorporate classified information to an unclassified system or network. Both instances constitute a reportable security violation.

(4) (**NEW**) (Added)(DAF) This includes if the on-installation cleared facility inquires as to whether or not the information involved is classified. All classification inquiries are to be deferred to the original classification authority or government customer for validation.

8.3.c.(1). **(REVISED**) (Added)(DAF) When the Installation Commander maintains oversight of on-installation cleared facilities, the supporting AFOSI detachment will take the actions required to assess the report for counterintelligence significance. (T-1) Servicing IPO personnel responsible for on-installation cleared facilities will ensure the on-installation cleared facility's final report is concise and contains, at a minimum, the impacted prime contract number or agreement number, level of classified information involved, referenced security classification guide, culpability(or not) and result of either compromise, suspected compromise, loss, or no compromise. (T-0).

8.3.c.(3). (**NEW**) (Added)(DAF) Servicing IPO personnel responsible for on-installation cleared facilities will either concur with the contractor's determination or propose an alternative determination for GCA review. (T-0).

8.3.c(4): (**NEW**) (Added)(DAF) Data spillage involving DAF authorized classified information systems and networks will be approved IAW DAF sanitization procedures. Servicing cybersecurity squadron personnel will provide written concurrence or non-concurrence to the servicing IPO for inclusion in the final reporting procedures to the GCA. Data spillage sanitization concurrence and non-concurrence procedures involving on-installation cleared facility unclassified contractor networks is as follows:

i. (**NEW**) (Added)(DAF) Servicing cybersecurity squadron personnel responsible for on-installation cleared facilities will require the on-installation cleared facility to self-certify, in writing through the contracting officer or contracting officer representative, to use appendix R of the DCSA Assessment & Authorization Process Manual (DAAPM) for sanitization procedures applicable to unclassified contractor owned networks and information system.

ii. (**NEW**) (Added)(DAF) Written contractor self-certification of sanitization will be forwarded to the servicing IPO for inclusion in the final reporting procedures.

iii. (**NEW**) (Added)(DAF) For cases where the on-installation cleared facility cannot meet the sanitization guidance found in appendix R of the DAAPM for its unclassified network(s) and/or information system(s), the servicing cybersecurity squadron will request the contractor provide this determination in writing.

iv. (**NEW**) (Added)(DAF) Servicing cybersecurity squadron personnel will submit the contractor's determination to the servicing IPO. and include a written request for the applicable GCA(s) to contact the contractor to approve contractor sanitization procedures occurring outside guidance found in the DAAPM, or successor document.

8.3.e. (**REVISED**) (Added)(DAF) When the Installation Commander provides oversight of on-installation cleared facilities, the IPO will route the final report of security violation to DCSA through MAJCOM/FLDCOM information protection channels and to SAF/OCS for further dissemination to relevant GCAs. The IPO will enter the report into the SAF/OCS designated repository. (T-1) Servicing IPO personnel responsible for on-installation cleared facilities will include either a concurrence or proposed alternative determination and indicate whether a weakness in security practices or procedures caused or permitted the loss, compromise or suspected compromise of classified information with the contractor's final report.(T-1)

8.3.g. (**NEW**) (Added)(DAF) For on-installation cleared facilities where the Installation Commander provides security oversight, if the Installation Commander determines on-installation cleared facility personnel should have their PCL suspended as a result of the security violation, the recommendation should be provided to DCSA with supporting documentation.

14.1.b. (**UPDATED**) (Added)(DAF) Information Protection Offices will maintain information regarding security reviews for on-installation cleared facilities in the SAF/OCS designated repository within 30 days of completed security reviews. (T-1) Information Protection Offices will provide completed security review reports to DCSA headquarters at dcsa.quantico.dcsa.mbx.isd-operations@mail.mil. (T-1)

14.2.a. (**NEW**) (ADDED)(DAF) Information Protection Offices providing oversight will request current facility information from the cleared facility at least 60 days ahead of the security review. This information will be used to determine the number of resources required to conduct the oversight and includes details about employee clearances, active contracts/programs, information systems, classified storage and holdings, classified visits/meetings, required reporting activities. Information Protection Offices will utilize a standard Request for Information provided by SAF/OCS.

(1) (**NEW**) (Added)(DAF) Servicing IPO personnel responsible for performing security oversight of on-installation cleared facilities must review the cleared facility in accordance with 32 CFR Part 117 and DCSA Industrial Security Letter (ISL) guidance. ISLs are available on DCSA.mil.

(2) (**NEW**) (Added)(DAF) Security reviews will include all information and facilities supporting collateral classified contracts to include non-DAF customers; generate a written report to DCSA within 20 duty days from the review completion IAW with this manual, unless otherwise documented; and provide correspondence to cleared facility management 20 duty days from the end date of the review, unless otherwise documented (T-1).

(3) (**NEW**) (Added)(DAF) Security reviews may consist of multiple team members and should include all cybersecurity and counterintelligence personnel required to support the on-installation cleared facility(ies). The IPO may also invite relevant GCA personnel to participate in the security reviews. The guidance contained in paragraph 14.b and all subparagraphs of 14.2.b. establish minimum review requirements, though not inclusive, until adequate training on the oversight of on-installation cleared facilities is provided by DCSA.

(4) (**NEW**) (Added)(DAF) Servicing IPO personnel are responsible for having knowledge of all NISPOM requirements.

b. In accordance with Paragraph 14.1 of this volume, DCSA or the Commander will assure that security reviews address, but not be limited to:

(1). (**NEW**) (Added)(DAF) Validate, at a minimum, all key management personnel information posted in NISS and verify all PCL eligibility information for KMP. If DAF personnel do not have the access rights in NISS to perform the validation, request the contractor to show you the company's NISS profile during the review or conduct validation with DCSA pre-security review.

(2) (**NEW**) (Added)(DAF) Validate, at a minimum and as applicable, exclusion resolutions for key management personnel and excluded business entities, as applicable, identified as excluded on the key management personnel listing as well as the effectiveness of any parent company exclusion resolution that may be in place due to parent/subsidiary

(3) (**NEW**) (Added)(DAF) FCL. Validate if all changed conditions have been reported through interviews and documentation review. The contractor is required to utilize NISS to report all changed conditions to DCSA. Refer to section 4.13 of this volume and the NISPOM for a description of reportable changed conditions.

(4) (**NEW**) (Added)(DAF) Validate if the contractor encountered any materiel changes to its SF328 or successor document if the on-installation cleared facility is the SF 328 signatory. Cleared facilities considered a division or branch location of a home office will not have its own SF 328, but rather fall under the home office SF 328. The SF 328 review is conducted at the home office level. Cleared facilities considered a cleared subsidiary may have their own SF328 or be a part of a consolidated SF 328 under the ultimate parent entity. If the cleared subsidiary has its own SF 328, this section applies. Until an automated solution is available to DAF personnel, contact DCSA to validate the business structure of the on-installation cleared facility and whether or not the contractor is a part of a consolidated SF328 at the home office level.

a. (**NEW**) (Added)(DAF) If the on-installation cleared facility is under a FOCI mitigation agreement, servicing IPO personnel are to ask questions and place information in the subsequent report:

(1) (**NEW**) (Added)(DAF) Identify the type of agreement; date of agreement; if the on-installation cleared facility is considered a subsidiary, verify if the subsidiary signed a document acknowledging the signatory FOCI mitigation agreement; and if there are any shared services of the home office FOCI mitigation agreement;

(2) (**NEW**) (Added)(DAF) Discuss what FOCI related information the facility reports to its Corporate Security entity at the home office and how the facility is in compliance with the FOCI mitigation agreement;

(3) (**NEW**) (Added)(DAF) If a NID is required, inquire about any outstanding NID requests and report back to DCSA, as applicable;

(4) (**NEW**) (Added)(DAF) Through employee interviews, validate if employees are aware of the government security committee members;

5) (**NEW**) (Added)(DAF) Inquire as to whether or not inside (as applicable) or outside directors visited the on-installation cleared facility;

6) (**NEW**) (Added)(DAF) For incoming visits from foreign parent or foreign affiliate personnel: Review the procedures on how visits are requested and approved; how visit records are kept; what visitation procedures are followed; review what types of visits occurred at the facility; the approval authority for the visits; if any visit requests were denied; inquire if any export authorizations were associated with the visit(s); and interview the hosts of the visits to determine whether or not the visitor was asking inappropriate questions;

(7) (**NEW**) (Added)(DAF) For outgoing visits from foreign parent or foreign affiliate personnel: Review what visits cleared facility personnel have taken to parent/affiliate companies;

(8) (**NEW**) (Added)(DAF) Inquire whether or not any social visits were reported to the home office;

(9) (**NEW**) (Added)(DAF) If applicable, review the cleared facility's electronic communication plan (ECP); verify the plan was approved by DCSA; document date of approval; inquire how the facility monitors interactions with foreign parent/affiliates (phone, email, fax); inquire how review of these records are maintained; and inquire whether or not there were any instances where communications where sent to or received by the cleared facility that violated the electronic communication plan or FOCI mitigation agreement;

(10) (**NEW**) (Added)(DAF) Review the facility's technology control plan (TCP) and whether or not it operates under a site-specific addendum approved by DCSA; inspect against the requirements of this document; through employee interviews, verify if contractor personnel are aware of who the Technology Control Officer is; validate if the cleared facility was involved with the release of any classified or export controlled information to a parent or affiliate company and if so, document the export license number; and inquire whether or not the cleared facility encountered any export violations in the past year;

(11) (**NEW**) (Added)(DAF) Inquire if the on-installation cleared facility has any personnel from either the foreign parent or affiliate companies physically present, permanently or temporarily, at the facility;

(12) (**NEW**) (Added)(DAF) Verify and validate how cleared facility personnel are trained on the FOCI mitigation agreement and how often briefings occur—security education briefings should include information on the ECP, TCP, visitation procedures, and export control, as applicable.

(5) (**NEW**) (Added)(DAF) Validate the following information, at a minimum, regarding the contractor's security education program through either a documentation review or contractor employee interviews:

a. (**NEW**) (Added)(DAF) Validate that the FSO completed the required training per DCSA guidance and if the contractor has procedures to provide cleared personnel with initial and annual security refresher briefings that include the topics of threat awareness, counterintelligence awareness, an overview of the information security classification system, reporting obligations (to include insider threat), cyber security training for all authorized classified information systems users (if applicable); and security procedures applicable to position requirement;

b. (**NEW**) (Added)(DAF) If the contractor is providing initial and annual insider threat training to personnel and if the training covers all NISPOM topic areas. NOTE: Training requirements can be combined with basic NISPOM security training requirements provided to contractor personnel;

c. (**NEW**) (Added)(DAF) If the FSO, Insider Threat Program Senior Official, and Insider Threat Program personnel have completed the required training for the position.

d. (**NEW**) (Added)(DAF) If the contactor provides CUI training when a classified contract provides provisions for the training;

e. (**NEW**) (Added)(DAF) If the contactor provides requisite insider threat training to both cleared contractor personnel and insider threat program personnel on an annual basis;

f. (**NEW**) (Added)(DAF) If the contractor has procedures on how to validate training completion and a system to maintain training records that reflect the most recent employee training date(s);

g. (**NEW**) (Added)(DAF) If the contractor has procedures on providing derivative classification training, as applicable, at least once every two years and include procedures to suspend an employee's derivative classification authority if not current on the training requirements;

h. (**NEW**) (Added)(DAF) If the contractor has procedures on debriefing employees (Industry may use the SF312 for this action, though it is not a policy requirement); and

i. (**NEW**) (Added)(DAF) If the contractor has procedures to brief/debrief personnel into NATO, COMSEC, or CNWDI and retains records IAW NISPOM requirements (as applicable).

(6) (**NEW**) (Added)(DAF) Verify, at a minimum:
(a) (**NEW**) (Added)(DAF) The contractor's procedures for employees requiring access to classified information during visits to other locations to include submitting electronic visit requests through DISS, or successor system, or

(b) (**NEW**) (Added)(DAF) Alternative method for visit request submission IAW NISPOM requirements in the event the electronic system is unavailable.

(7) (**NEW**) (Added)(DAF)) Verify the following, at a minimum: If the contractor verifies U.S citizenship using original or certified copies of original documentation; procedures for completing the electronic version of the SF 86 (or equivalent system), electronic fingerprinting, and any pre-employment clearance actions (e.g. maintains written commitment documentation); employs any consultants (if applicable) to include a review of the executed consultant agreement. For security administration purposes, a consultant will be considered an employee of the using contractor for compliance. The consultant and the using contractor will jointly execute the consultant agreement setting forth respective security responsibilities. The contractor will retain an original signed copy of the agreement. Refer to the NISPOM for consultant agreement requirements.

(a) (**NEW**) (Added)(DAF) Validate, at a minimum, that contractor employees are provided written notification that the review of the SF 86 (or equivalent) by the FSO or other contractor employee is for adequacy and completeness.

(b) (**NEW**) (Added)(DAF) Validate, at a minimum, the contractor is providing the contractor employee written notification that SF 86 (or equivalent) information will be used for no other purpose within the entity, that the information provided by the employee is protected by the "Privacy Act of 1974, as amended" and that the Privacy Act notice included in the SF 86, including the routine uses for which this information can be disclosed, applies to this information collection.

(c) (**NEW**) (Added)(DAF) Validate, at a minimum, the need for PCLs will be validated through employee interviews to ensure the contractor is not creating a pool of cleared employees. Ensure cleared employees are actively accessing classified information. Validate, as applicable, if the contractor has any current LAAs on file and if personnel issued a LAA are only accessing classified information within the conditions of the LAA.

(d) (**NEW**) (Added)(DAF) Validate, at a minimum, that the contractor is annotating and maintaining the accuracy of their employee's records in the system of record for contractor eligibility (e.g. DISS or successor system) including verifying all contractor employees have up to date investigations ; properly executed SF312s; refusals to execute SF312s; classified access granted commensurate with granted classified eligibility

(8) (**NEW**) (Added)(DAF) Verify, at a minimum, that the contractor:

(a) (**NEW**) (Added)(DAF) Maintains valid/active DD Form 254s that communicate the appropriate classification guidance;
(b) (**NEW**) (Added)(DAF) Properly marks classified holdings;

(c) (**NEW**) (Added)(DAF) Established procedures for the control of classified working papers by dating the working papers when created; marking each page with the highest classification level and the working paper designation; destroy when no longer needed; and mark in the same manner as a finished document when retained for more than 180 days; and

(d) (**NEW**) (Added)(DAF) Obtains public release authorization, as applicable, from its customer for all unclassified information associated with classified contracts.

(9) (**NEW**) (Added)(DAF) Validate, at a minimum and if applicable, whether or not the contractor:

(a) (**NEW**) (Added)(DAF) Issues classified subcontracts;

(b) (**NEW**) (Added)(DAF) Has procedures on validating FCL information of subcontractors;

(c) (**NEW**) (Added)(DAF) Is providing the subcontractor adequate security classification guidance via the subcontract DD Form 254.

(d) (**NEW**) (Added)(DAF) Obtains GCA approval for subcontractor retention of classified information associated with a completed contract if retention will go beyond two years.

(e) (**NEW**) (Added)(DAF) Obtains GCA approval prior to subcontracting COMSEC, FGI, CNWDI, SAP, SCI (including intelligence information), NATO, or TEMPEST requirements.

(10) (**NEW**) (Added)(DAF) The following will be reviewed, at a minimum, through documentation review and/or contractor employee interviews regarding the contractor's insider threat program IAW DCSA requirements that the contractor:

(a) (**NEW**) (Added)(DAF) Appointed an Insider Threat Program Senior Official (ITPSO), who is a U.S. citizen; an employee of the company; identified on the Key Management Personnel list; completed all ITPSO required training; and possesses classified eligibility commensurate with the level of the facility clearance (the FSO can also be the ITPSO);

(b) (**NEW**) (Added)(DAF) A corporate family may choose to establish a corporate-wide insider threat program with one senior official appointed to establish and execute the program. Each cleared legal entity in the corporate family using the corporate-wide ITPSO must separately appoint that person as the ITPSO for that cleared legal entity. When a corporate family appoints a single ITPSO, that individual must be able to effectively manage the insider threat requirements for each entity for which they are appointed or maintain a record of the individuals at each cleared facility who are trained to support and implement insider threat program requirements;

(c) (**NEW**) (Added)(DAF) Has a self-certified Insider Threat Program plan and whether or not the ITPSO has the authority to implement the plan at the contractor location;

(d) (**NEW**) (Added)(DAF) Provides both initial and annual insider threat training to personnel; maintains a record of the training; and if the training covers all NISPOM topic areas (Training requirements can be combined with basic NISPOM security training requirements provided to contractor personnel);

(e) (**NEW**) (Added)(DAF) Has an effective insider threat program which can be demonstrated by having:

1. (**NEW**) (Added)(DAF) An ITPSO trained on applicable legal, civil liberties, and privacy policies and requirements applicable to insider threat programs and who is integrated with, or coordinates with, the company's legal counsel and civil liberties and privacy officials ensuring all program activities are conducted within applicable laws, whistleblower protections, civil liberties, and privacy protections;

2. (**NEW**) (Added)(DAF) A program that has the capability to gather, integrate, and report relevant and credible information within the national security guidelines contained in Security Executive Agent Directive (SEAD) 4, and implementing DoD guidance;

3. (**NEW**) (Added)(DAF) Procedures in place to gather information across the company (e.g. human resources, security, information assurance, legal) commensurate with the size and complexity of the company;

4. (**NEW**) (Added)(DAF) The ITPSO and personnel performing duties related to the insider threat program receive regular, timely access to all relevant information to identify violations, areas of concern, or potential insider threat matters to include procedures for timely resolution; and

5. (**NEW**) (Added)(DAF) A process for a self-assessment of its insider threat plan (can be combined with the traditional self-assessment requirement).

(11) (**NEW**) (Added)(DAF) Validate, at a minimum, the contractor implemented the following self-inspection requirements:

(a) (**NEW**) (Added)(DAF) Contractors will review their security programs on a continuing basis and conduct a formal self-inspection at least annually and at intervals consistent with risk management principles;

(b) (**NEW**) (Added)(DAF) Self-inspections will include the review of the classified activity, classified information, classified information systems, conditions of the overall security program, and the insider threat program. They will have sufficient scope, depth, and frequency, and will have management support during the self-inspection and during remedial actions taken as a result of the self-inspection. Self-inspections will include the review of samples representing the contractor's derivative classification actions, as applicable;

(c) (**NEW**) (Added)(DAF) The contractor will retain the formal report for review until after the next security review is completed; and

(d) (**NEW**) (Added)(DAF) (Added) (DAF) The Senior Management Official at the cleared facility will annually certify, in writing, that a self-inspection has been conducted, that other KMP have been briefed on the results of the self-inspection, that appropriate corrective actions have been taken, and that management fully supports the security program at the cleared facility in the manner as described in the certification.

(13).(a) (**NEW**) (Added)(DAF) The below will be validated, at a minimum, to ensure the contractor implemented the following:

1. (**NEW**) (Added)(DAF) Review contractor procedures for establishing need-to-know;

2. (**NEW**) (Added)(DAF) Review contractor procedures for the positive identification of visitors; approving visits, identifying and controlling the access and movement of incoming visitors, and precluding unauthorized access;

3. (**NEW**) (Added)(DAF) Ensure the contractor continues to provide security oversight of employees resident at USG locations; and

4. (**NEW**) (Added)(DAF) Ensure USG employees or other contractor employees meeting the long term visitor threshold at the cleared facility follow the host contractor security procedures, unless the USG employees are resident in a USG designated space under the control of USG personnel (e.g. leases space at the cleared facility for USG use).

(b) (**NEW**) (Added)(DAF) Classified Materiel Controls. The below will be validated, at a minimum, that the contractor:

1. (**NEW**) (Added)(DAF) Conducts end of day security checks;

2. (**NEW**) (Added)(DAF) Has perimeter control procedures in place (e.g. inspection of personnel/signage);

3. (**NEW**) (Added)(DAF) Developed emergency procedures for safeguarding classified information;

4. (**NEW**) (Added)(DAF) Maintains procedures for both incoming and outgoing classified mail;

5. (**NEW**) (Added)(DAF) Has approval to use commercial carriers IAW DCSA guidance (if applicable);

6. (**NEW**) (Added)(DAF) Briefs contractor personnel on couriering procedures (if applicable);

7. (**NEW**) (Added)(DAF) Maintains an information management system;

8. (**NEW**) (Added)(DAF) Implements top secret material controls (if applicable) including:

(a) (**NEW**) (Added)(DAF) The designation of Top Secret Control Officials to receive, transmit, and maintain access and accountability records of top secret information;

(b) (**NEW**) (Added)(DAF) Conduct an annual inventory of top secret information and material;

(c) (**NEW**) (Added)(DAF) Establish a continuous receipt system for the transmittal of top secret information within and outside the contractor location, number each item of top secret material, in series and place the copy number on top secret documents, regardless of media and on all associated transaction documents;

(d) (**NEW**) (Added)(DAF) Establish a record of top secret material when it is completed as a finished document, retained for more than 180 days after creation regardless of the stage of development, and transmitted outside of the contractor location; and

(e) (**NEW**) (Added)(DAF) Establish procedures for the destruction of top secret material by two authorized persons; establish destruction records for top secret material and maintain the records for two years or IAW government customer requirements.

9. (**NEW**) (Added)(DAF) Maintains current open storage area requirements, intrusion detection system requirements, and coordinates all proposed changes to existing open storage areas with the servicing IPO; and

10. (**NEW**) (Added)(DAF) Changes combinations when the equipment is placed into use, whenever a person with knowledge of the combination no longer requires access (unless other sufficient controls exist to prevent access to the lock), or whenever the combination has been subject to possible unauthorized disclosure.

c. (**NEW**) (Added)(DAF) When Installation Commanders retain oversight of on-installation cleared facilities, servicing IPO personnel will document all NISPOM non-compliance items and security ratings using guidelines established by DCSA and posted at www.dcsa.mil. (T-1).

14.5 (**NEW**) (Added)(DAF) When Installation Commanders retain oversight of on-installation cleared facilities, the security review report will follow the format in appendix 14A until DCSA provides the DAF tools and a template. (T-0).

Administrative Changes to AFMAN 16-1406, *National Industrial Security Program: Industrial Security Procedures for Government Activities*

OPR: SAF/AAZO

References throughout to “DoDM5220.22, Volume 2” are hereby changed to “DoDM5220.32, Volume 1.”

References throughout to “DoD5220.22-M” are hereby changed to “32CFR Part 117.”

References throughout to “Enterprise Protection Risk Management (EPRM) tool” are hereby changed to “Management Internal Control Toolkit (MICT).”

References throughout to “EPRM” are hereby changed to “MICT.”

“EPRM” will hereby be removed from G.1. Acronyms.

“MICT – Management Internal Control Toolkit” will hereby be added to G.1. Acronyms.

25 March 2022

BY ORDER OF THE SECRETARY OF THE AIR FORCE

DEPARTMENT OF DEFENSE MANUAL 5220.22 Volume 2

AIR FORCE MANUAL 16-1406, Volume 2

8 MAY 2020

Operations Support

NATIONAL INDUSTRIAL SECURITY PROGRAM: INDUSTRIAL SECURITY PROCEDURES FOR GOVERNMENT ACTIVITIES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: **Publications and forms are available for downloading or ordering on the e-Publishing web site at www.e-Publishing.af.mil**

RELEASABILITY: **There are no releasability restrictions on this publication**

OPR: SAF/AAZO

Certified by: SAF/AAZ (Mr. William E. MacLure)

Supersedes: AFI 16-1406, 25 August 2015

Pages: 176

This publication implements the industrial security portion of the security enterprise defined in Air Force Policy Directive (AFPD) 16-14, *Security Enterprise Governance*. This Air Force Manual (AFMAN) is prepared as an overprint to Department of Defense Manual (DoDM) 5220.22, Volume 2, *National Industrial Security Program: Industrial Security Procedures for Government Activities*. DoDM 5220.22, Volume 2 is printed word-for-word in regular font without change. The Air Force supplemental material is printed in bold font and indicated by "(Added)(AF)." This supplement provides guidance for implementing the National Industrial Security Program (NISP) and is applicable to the Regular Air Force, the Air National Guard, the Air Force Reserve, all civilian personnel of each Air Force component, and contractor personnel performing under the terms of a properly executed classified contract with performance on an Air Force installation or within an Air Force facility, except where noted otherwise in the contract. This AFMAN may be supplemented at any level, but all supplements will be routed to the office of primary responsibility (OPR) prior to certification and approval. Refer recommended changes and questions about this publication to the OPR listed above using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate chain of command. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, and T-3") number following the compliance statement. See Air Force Instruction (AFI) 33-360, *Publications and Forms Management,* Table 1.1 for a description of the authorities associated with the tier numbers. Submit requests for waivers through the chain of command to the appropriate tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items. Ensure all records created as a

result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Information Management System.

SUMMARY OF CHANGES

This document has been substantially revised and needs to be completely reviewed. This publication has been changed from an Air Force Instruction to an Air Force Supplement to the Department of Defense Manual. It incorporates new guidance from the Under Secretary of Defense for Intelligence, which provides updated guidance regarding the NISP.

DoD Manual 5220.22, Volume 2

National Industrial Security Program: Industrial Security Procedures for Government Activities

Originating Component:	Office of the Under Secretary of Defense for Intelligence
Effective:	August 1, 2018
Releasability:	Cleared for public release. Available on the Directives Division Website at http://www.esd.whs.mil/DD/.
Incorporates and Cancels:	DoD 5220.22-R, "Industrial Security Regulation," December 4, 1985 DoD 5220.22-C, "Carrier Supplement to Industrial Security Manual for Safeguarding Classified Information," October 1, 1986 Under Secretary of Defense for Intelligence Memorandum, "Authority to Suspend Contractor Personnel Security Clearances," May 13, 2009
Approved by:	Joseph D. Kernan, Under Secretary of Defense for Intelligence **Mr. Anthony P. Reardon, Administrative Assistant**

Purpose: This manual is composed of several volumes, each containing its own purpose. In accordance with the authority in DoD Directive (DoDD) 5143.01:

- This manual implements policy, assigns responsibilities, establishes requirements, and provides procedures, consistent with Executive Order (E.O.) 12829, DoD Instruction (DoDI) 5220.22, and E.O. 10865, for the protection of classified information that is

disclosed to, or developed by contractors, licensees, and grantees (referred to in this manual as contractors) of the U.S. Government (USG).

- This volume prescribes industrial security procedures and practices applicable to USG activities using the DoD as their cognizant security agency (CSA). This ensures maximum uniformity and effectiveness in DoD implementation of the National Industrial Security Program (NISP) in accordance with E.O. 12829.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This volume applies to:

a. OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively as the "DoD Components").

b. Those non-DoD executive branch departments and agencies (referred to collectively as the "non-DoD Components") identified in DoD 5220.22-M. These non-DoD Components have entered into agreements with the Secretary of Defense (SecDef), pursuant to E.O. 12829, under which DoD acts as the CSA, to provide security oversight services to ensure the protection of classified information disclosed to or generated by contractors.

c. When the term "Component" is used in this volume, it is referring to both DoD and non-DoD Components.

d. When the term "Government Contracting Activity (GCA)" is used in this volume, it will refer to contracting activities of both DoD and non-DoD Components.

d. (Added)(AF) GCA is defined in paragraph G.2. of this volume. The GCA consists of a multifunctional team with numerous responsibilities as defined in this volume.

(1) This manual does not limit in any manner the authority of the SecDef, the Secretaries of the Military Departments, or the Component heads to grant access to classified information under the cognizance of their department or agency to any individual designated by them. The granting of such access is outside the scope of the NISP and will be governed by E.O. 13526 and applicable disclosure policies.

(2) This volume does not restrict the authority of a Component or a GCA to limit, deny, or revoke access to classified information under its statutory, regulatory, or contractual jurisdiction and does not apply to:

e. Contractors and companies in process for facility security clearances (FCLs), as those are subject to the requirements of DoD 5220.22-M and the security requirements of their contracts.

f. The protection of national intelligence and access to intelligence sources and methods, including sensitive compartment information (SCI). The Director of National Intelligence (DNI) has the authority to prescribe standards for the protection of national intelligence and access to intelligence sources and methods, including SCI, pursuant to section 3024 of Title 50, United States Code (U.S.C.) as implemented in Intelligence Community Directive (ICD) 700. Eligibility for access to SCI must be verified through applicable SCI channels.

g. Eligibility for access to Special Access Program (SAP) information must be verified through applicable SAP channels in accordance with DoDI 5205.11.

1.2 POLICY It is DoD policy that:

a. The SecDef serves as the Federal Executive Agent for inspecting and monitoring contractors under the NISP in accordance with E.O. 12829. The SecDef may prescribe such specific requirements and procedures for Components and their GCAs to follow to protect classified information that may be disclosed, or has been disclosed, to current, prospective, or former contractors, licensees, or grantees of USG agencies.

b. The SecDef is authorized by E.O. 12829 to enter into agreements with any other Executive Branch department or agency to provide industrial security services required for safeguarding classified information disclosed to contractors by these non-DoD Components.

c. As a CSA, the DoD will establish, in accordance with E.O. 12829 and DoDI 5220.22, policies, procedures, and practices to be followed by Components and their GCAs for the effective protection of classified information provided to industry, including foreign government information (FGI) that the USG is obligated to protect in the interest of national security.

d. In accordance with E.O. 12829, DoD, the Office of the DNI, Department of Energy (DOE), the Nuclear Regulatory Commission, and the Department of Homeland Security (DHS) are the only Executive Branch agencies that are authorized to function as CSAs for the NISP. Pursuant to Part 2004 of Title 32, Code of Federal Regulations (CFR), CSAs are responsible for the security of classified contracts and activities under their purview; oversight of contractors under their security cognizance; and ensuring that redundant and duplicative security review and audit activity of contractors is held to a minimum, including such activity conducted at contractor facilities where multiple CSAs have equities.

e. Security eligibility for contractor personnel requiring access to classified information will be determined in accordance with the established standards and criteria in DoDD 5220.6.

1.3. INFORMATION COLLECTIONS. DD Form 254, "Department of Defense Contract Security Classification Specification," referred to in paragraph 3.4.a of this volume, is assigned Office of Management and Budget (OMB) control number 0704-0567 for contract security classification specification requirements in accordance with Volume 2 of DoD Manuel (DoDM) 8910.01.

a. The reports on violations to the Director, Information Security Oversight Office (ISOO), referred to in Paragraph 3.9 of this volume, are exempt from licensing in accordance with Paragraph 8.a.(2)(c) of Enclosure 3 of Volume 2 of DoDM 8910.01.

b. The requests for FCL, referred to in Paragraph 4.3 of this volume, are assigned OMB control number 0704-0571, in accordance with Volume 2 of DoDM 8910.01.

c. The collection and maintenance of contractor FCL records, referred to in Appendix 4a of this volume, is assigned OMB control number 0704-0571, in accordance with Volume 2 of

DoDM 8910.01.

d. The reporting of suspicious contacts, referred to in Paragraph 8.2 of this volume, is exempt from licensing in accordance with Paragraph 8.a.(2)(d) of Enclosure 3 of Volume 2 of DoDM 8910.01.

e. The Security Review Report, referred to in Appendix 14A of this volume, is exempt from licensing in accordance with Paragraph 8.a.(2)(c) of Enclosure 3 of Volume 2 of DoDM 8910.01.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE (USD(I)). In accordance with DoDD 5143.01 and DoDI 5220.22, the USD(I):

a. Oversees policy and management of the NISP.

b. Directs, administers, and oversees the NISP to ensure that the program is efficient and consistent.

c. In accordance with E.O. 12829, reports intra- or inter-agency agreements that create redundant and duplicative security reviews, inspections, or audit activity by other CSAs to the Director, ISOO.

d. Considers and, as warranted:

(1) Approves or disapproves any requests for exceptions to this volume;

(2) Approves or disapproves any requests for exceptions to DoD 5220.22-M as described in Paragraph 2.2.x of this volume that apply to more than one contractor location, and;

(3) Coordinates with the Under Secretary of Defense for Policy (USD(P)) on all matters involving requests for exception to this volume or DoD 5220.22-M that would affect international agreements, the international security requirements of DoD international cooperative projects and programs, including those relating to FGI and international issues, and on all matters affecting international technology transfer.

e. May delegate the authorities in Paragraph 1.1.d.(1) - (3) to a DoD Official.

2.2. DIRECTOR, DEFENSE SECURITY SERVICE (DSS). Under the authority, direction, and control of the USD(I), in accordance with DoDI 5220.22 and DoDD 5105.42, and in addition to the responsibilities in DoDD 5240.02, DoDD 5240.06 (when required by contract)), DoDD 5205.16 and in Paragraph 2.7 of this volume, the Director, DSS:

2.2. (Added)(AF) The Secretary of Defense issued the memorandum, *Renaming the Defense Security Service as the Defense Counterintelligence and Security Agency*, 20 June 2019 with the mission to secure classified and sensitive information and technology in the U.S. industrial base against attack and compromise, ensure the federal and contractor workforce can be trusted with sensitive and classified information, and preserve military readiness and warfighting capabilities by identifying and defeating threats presented by and to the defense supply chain.

a. Budgets and funds the NISP.

a. (Added)(AF) The Defense Counterintelligence and Security Agency (DCSA) budgets and funds only for NISP investigative requirements. DCSA is not tasked with or empowered to resource requirements outside of the NISP (e.g., credentialing investigations for logical or physical access, investigative requirements for sensitive positions not requiring access to classified information, etc.). Resourcing for non-NISP requirements is the responsibility of the requiring activity.

b. Administers the NISP as a separate program element on behalf of the GCAs, to include providing security oversight as the cognizant security office (CSO) on behalf of the GCAs, for U.S. contractors and U.S. companies in process for an FCL in accordance with this manual. DSS is relieved of this oversight function for DoD SAPs when the SecDef or the Deputy Secretary of Defense approves a carve-out provision for a DoD SAP in accordance with the provisions described in Section 3 of this volume.

c. Executes intra- and inter-agency agreements as necessary to avoid redundant and duplicative security reviews or inspections, including such activity conducted at contractor facilities by other CSAs. Notifies the Office of the Under Secretary of Defense for Intelligence CI and Security (OUSD(I) CI&S) of unresolved instances of redundant or duplicative security reviews, inspections or audit activity.

d. Trains GCA personnel (i.e., contracting officers, contracting officer representatives, industrial security personnel and others performing security duties) on the requirements of this manual and of industrial security matters as required or upon request, including insider threat education and awareness.

e. Provides, as authorized in support of cleared contractors and within DSS, CI assistance or support, in accordance with DoDD 5105.42.

e. (Added)(AF) All CI assistance and support within the Air Force is provided by the Air Force Office of Special Investigations (AFOSI) in accordance with AFPD 71-1, *Criminal Investigations and Counterintelligence*.

f. Leverages the security expertise of contractors by granting self-approval authority to a contractor's designated personnel who meet specific criteria demonstrating appropriate security education training and awareness (SETA) applicable to a specific topic or area of industrial security in accordance with Paragraph 9.2.b.(6) of this volume.

g. Establishes a professional career development program for DSS personnel to ensure the continuing effectiveness of DSS oversight of NISP contractors.

h. Develops authorizing official (AO) guidance for contractor information systems to process classified information for those contractors under DSS security cognizance and coordinates the guidance with OUSD(I) CI&S and the National Industrial Security Program Policy Advisory Committee (NISPPAC) prior to publication. If requested, provides the DoD GCAs, and the Office of the Chief Information Officer of the Department of Defense with the published AO guidance for their reference about contractor information systems that process

classified information under DSS security cognizance.

i. Determines, in coordination with the General Counsel of the Department of Defense (GC DoD), whether action should be taken to suspend a contractor employee's clearance eligibility in accordance with the provisions of DoDD 5220.6 and Section 5 of this volume.

j. In accordance with DoDD 5105.42 and the provisions in Section 12 of this volume, directs the proper implementation by DSS of the requirements in parts 120-130 of Title 22, CFR, also known as the International Traffic in Arms Regulations (ITAR); DoDD 5230.11; bilateral security agreements; guidance from the USD(P) pursuant to DoDD 5111.1 and DoDD 5230.20; program-specific agreements with allies and other friendly countries; and North Atlantic Treaty Organization (NATO) requirements implemented by United States Security Authority for NATO Affairs Instruction 1-07 and DoDI 5210.60, as described in DoD 5220.22-M for the protection of U.S. classified information and FGI to which U.S. contractors may have access.

k. In consultation with the Office of the Under Secretary of Defense for Policy (OUSD(P)), maintains a complete set of copies of the security agreements that have been negotiated with various foreign governments or international organizations (referred to collectively in this volume as "foreign governments") and allows contractors cleared to the appropriate level and having a need-to-know to view the applicable agreement at a DSS office.

l. Develops appropriate changes to maintain the volumes of this manual in a current and effective basis in accordance with DoDI 5025.01. Proposed changes to these documents will be forwarded to the OUSD(I) CI&S.

m. Prepares, coordinates, and publishes industrial security letters (ISLs) with the approval of the USD(I).

n. Establishes and maintains a system for timely and effective communication with the GCAs and the NISP contractors.

o. Provides information, upon GCA request, to assist with the review of the security aspects of GCA classified contracts.

p. Provides updates to the FCL and safeguarding capability status of specific facilities upon request.

q. Maintains a DoD database (currently the Industrial Security Facilities Database (ISFD)) for all current, pending, and recently terminated FCLs with the associated oversight activity and resulting actions.

q. (Added)(AF) Effective October 8, 2018, the National Industrial Security System (NISS) replaced ISFD as the system of record for FCL information.

r. Maintains a record of GCA or contractor requests and responses for facility security

clearance assurances (FCLA) or personnel security clearance assurances (PCLSA) for foreign companies and individuals.

s. Maintains the forms and associated instructions in this volume in accordance with DoD 7750.07-M.

t. Maintains an industrial security operating manual with any detailed procedures and direction for DSS personnel in the execution of the industrial security mission, consistent with the requirements of this manual.

u. Provide procedures and any subsequent updates to any DoD Components performing FCL oversight (i.e., commanders or heads of USG-controlled installations who have retained oversight of any cleared facility on the installation) to assure that they know where and to whom at DSS to submit updates about any pending or on base cleared contractor facilities under their cognizance.

v. Develops procedures that provide for:

(1) When and how notices of proposed or final FCL revocation or denial decisions will be communicated to contractors.

(2) The content of those notices.

(3) Designation of which DSS officials will be authorized to revoke or deny an FCL.

(4) Administrative requests for reconsideration or appeals that contractors can request after an FCL has been revoked or denied.

(5) Required coordination with OUSD(I) and the Office of the Deputy General Counsel for Intelligence, if the procedures provide that requests for reconsideration or appeals from FCL revocations or denials may be made to the USD(I) or an official on the OUSD(I) staff outside of DSS.

w. Retains the Standard Form (SF) 312, "Classified Information Nondisclosure Agreement," executed by all contractor personnel cleared for access to classified information under DoD NISP security cognizance. DoD 5220.22-M provides guidance to contractor personnel regarding the SF 312 execution and debriefing requirements. Blank copies of the SF 312, which includes revisions made by the Office of the Director of National Intelligence to reflect language required by two statutes: Public Law 112-74 and Public Law 112-199 can be found at http://www.gsa.gov/portal/forms/download/116218.

x. Considers, and as warranted, approves or disapproves requests for exceptions to DoD 5220.22-M in consultation with affected GCAs for specific contractor locations and for specific periods of time (such as, for the duration of a contract).

y. Coordinates with the USD(P) and the Under Secretary of Defense for Acquisition,

Technology and Logistics (USD(AT&L)) on matters under their cognizance that impact the NISP consistent with this manual.

2.3. USD(P). In accordance with DoDD 5111.1, the USD(P):

a. Develops policy and procedures for the safeguarding, access control, and transfer of classified information subject to export control pursuant to the ITAR.

b. Develops policy and procedures for the safeguarding, access control, and transfer of NATO information consistent with United States Security Authority for NATO Affairs Instruction 1-07.

c. Develops policy and procedures for the safeguarding, access control, and transfer of classified information subject to bilateral and multinational security and program-specific agreements with foreign governments.

d. Develops policy and procedures for the negotiation of international agreements and the foreign disclosure, technology control, and security requirements for international programs. When such agreements are executed, provide DSS with a copy.

e. Establishes qualifications and standards and provides guidance for the content of courses of instruction that are to fully train attendees on national and DoD policies on foreign disclosure, technology control, and security requirements for DoD international programs, consistent with DoDD 5230.11 and the October 22, 1999 Deputy Secretary of Defense Memorandum.

2.4 USD(AT&L). In accordance with DoDD 5134.01, consistent with the responsibilities in DoDI 5220.22, the USD(AT&L):

2.4. (Added)(AF) On February 1, 2018, the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) was reorganized into the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) and Under Secretary of Defense for Research and Engineering (USD(R&E)).

a. Advises the USD(I) on the development and implementation of NISP policies, in accordance with DoDI 5220.22.

b. Ensures DoD GCAs establish and maintain a record of the current and legitimate need for access to classified information by contractors in the defense industrial base.

2.5. DIRECTOR, WASHINGTON HEADQUARTERS SERVICES (WHS). Under the authority, direction, and control of the Deputy Chief Management Officer of the Department of Defense and in accordance with Security Executive Agent Directive 4, DoDI 5200.02, DoDD 5220.6, DoDM 5200.02, the October 22, 2012 Director of National Intelligence Memorandum, and the May 3, 2012 Deputy Secretary of Defense Memorandum, the Director, WHS, conducts

national security eligibility adjudications for access to classified information by contractor personnel under DSS cognizance. See Sections 4, 5, and 8 of this volume for additional guidance.

2.6. GC DOD. In accordance with DoDD 5220.6, DoDD 5145.01, and DoDI 5145.03, the GC DoD:

a. Provides advice and guidance to the DoD as to the legal sufficiency of procedures and standards established by this manual.

b. Ensures that DoD NISP policies, standards, and procedures are in accordance with all applicable E.Os., ICDs, court decisions, and statutory requirements.

c. Ensures that all relevant statutes, E.Os., and court decisions are reviewed on a continuing basis and that analysis of the foregoing is accomplished and disseminated to DoD NISP management authorities.

d. Performs functions relating to the NISP in accordance with DoDD 5220.6, including maintenance and oversight of the Defense Office of Hearings and Appeals (DOHA).

2.7. DOD COMPONENT HEADS. In accordance with DoDI 5220.22 and DoDD 5205.16, the DoD Component heads:

a. Oversee compliance by the Component's personnel with applicable procedures identified in this volume.

a. (Added)(AF) The Chief, Information Protection will perform this responsibility on behalf of the Installation Commander. (T-1) The Air Force Inspector General will oversee compliance across the Air Force in accordance with this volume. (T-1)

b. May augment this volume by prescribing more detailed procedures for Components and their GCAs as may be required for particular circumstances, provided they are consistent with this volume.

b. (Added)(AF) This publication may be supplemented by Major Commands (MAJCOMs) and Direct Reporting Units (DRUs); however, drafts must be reviewed by this publication's OPR prior to publication. (T-1)

c. Ensure that the Component or its GCA industrial security personnel, and others performing security duties (i.e., contracting officers or contractor officer representatives) complete appropriate security education and training.

c. (Added)(AF) Individuals assigned as activity security manager will possess the rank/grade and training requirements identified in AFI 16-1404, *Air Force Information Security Program*. (T-0) The activity security manager, or designee, will ensure

appropriate training for others performing security duties (e.g., contracting officers or contracting officer representatives, etc.). (T-1) Special emphasis should be made to ensure contracting officers and requiring officials receive sufficient training to effectively administer and oversee classified contracts. There are numerous resources available to aid in these training requirements available from the Center for the Development of Security Excellence online at www.cdse.edu or www.dcsa.mil.

d. Provide oversight of contractor personnel visiting or working on USG-controlled installations.

d. (Added)(AF) Host wing Information Protection Offices will perform oversight of cleared facilities and visitor groups on Air Force installations on behalf of the Installation Commander unless the Installation Commander delegates oversight to a tenant Information Protection Office in writing. (T-1) A memorandum of agreement or base services support agreement may serve as the written delegation of responsibilities. Cleared facilities are evaluated in accordance with DoD 5220.22-M, *National Industrial Security Program Operating Manual*. Visitor groups are integrated into the installation's information security program and evaluated as part of the installation's oversight programs.

e. Review the security aspects of classified contracts with contractors as needed.

e. (Added)(AF) Contracting officers or designees, with the assistance of requirements owners (e.g., program management), will assist contractors regarding the security aspects of classified contracts as needed. (T-1)

f. Propose changes to the volumes of this manual as deemed appropriate and provide them to the OUSD(I) CI&S.

g. Notify the OUSD(I) CI&S of any substantive issues prior to public meetings of the NISPPAC or NISPPAC working group meetings to facilitate a coordinated DoD position.

h. Establish procedures to report in the DoD personnel security system of record information that becomes known to the GCA or to other elements of the respective Component that adversely reflects on the integrity or character of a contractor or contractor employee; that suggests that his or her ability to safeguard classified information may be impaired; that his or her access to classified information clearly may not be in the interest of national security or the contractor employee poses an actual or potential insider threat.

(1) (Added)(AF) Commanders shall report to the DCSA Vetting Risk Operations Center (VROC) and to the Department of Defense Consolidated Adjudications Facility (DoD CAF), any adverse or questionable information that comes to his or her attention, concerning a contractor employee who has been cleared, or is in the process of being cleared, for access to classified information, which may indicate that such access is not clearly consistent with the national interest. (T-0) Commanders shall also provide this notification to the servicing Information Protection Office and to other relevant security

authorities (e.g., Special Security Officer, Program Security Officer (PSO), Government SAP Security Officer) when appropriate. (T-1)

(2) (Added)(AF) If the commander can confirm that the company's Facility Security Officer notified the DCSA VROC and the DoD CAF, additional notification is not required. (T-3)

(3) (Added)(AF) Until such time as an automated solution is developed to provide simultaneous notification to the DCSA VROC and the DoD CAF, Commanders are responsible for ensuring both notifications are accomplished.

(a) (Added)(AF) Commanders will provide initial notification to the servicing Information Protection Office who will further notify DCSA VROC and the DoD CAF. (T-1) Commanders will ensure notification procedures to the servicing Information Protection Office are developed locally. (T-1)

(b) (Added)(AF) The Information Protection Office will provide initial notification to DCSA VROC via their notification mailbox at dss.ncr.dss-dvd.mbx.askvroc@mail.mil and ensure these notifications are sanitized such that they do not reveal protected information or encrypt the email when sending. (T-1) If sending a sanitized notification, DCSA will follow-up receipt of the email with additional contact information where a complete report can be made.

(c) (Added)(AF) The Information Protection Office will provide notification to the DoD CAF through the Joint Personnel Adjudication System (JPAS) or successor system. (T-1)

(d) (Added)(AF) Commanders shall ensure notifications to DCSA VROC and the DoD CAF include relevant information in accordance with DoDM5200.02_AFMAN16-1405, *Air Force Personnel Security Program*. (T-1)

2.8. (Added)(AF) AIR FORCE INDUSTRIAL SECURITY PROGRAM.

a. (Added)(AF) Senior Agency Official. The Administrative Assistant to the Secretary of the Air Force (SAF/AA), is the Secretary of the Air Force appointed authority responsible for oversight of information protection for the Air Force security enterprise. See Headquarters Air Force Mission Directive 1-6.

b. (Added)(AF) The Director, Security, Special Program Oversight and Information Protection (SAF/AAZ) serves as the principal advisor to SAF/AA for information protection. SAF/AAZ provides strategic policy and addresses the equities within the functional portfolio related to information protection to include the Air Force industrial security, information security, and personnel security programs.

c. (Added)(AF) The Security Program Executive (SPE) is appointed by the MAJCOM, DRU, or Field Operating Agency (FOA) commander in accordance with AFPD 16-14.

The SPE will provide oversight of each respective MAJCOM, DRU, or FOA information protection program. (T-1) As used throughout this volume, the term MAJCOM includes DRU and FOA. At a minimum, the SPE will:

(1) (Added)(AF) Provide oversight of the industrial security program within their command and enforce standards to ensure classified information entrusted to industry is protected. (T-1)

(2) (Added)(AF) Approve or make recommendations as appropriate regarding waivers, exceptions, or deviations to policy and submit them to the appropriate organizational entity as required by this volume. (T-1)

(3) (Added)(AF) Ensure the security posture of contractor operations on Air Force installations is assessed and report the information to the appropriate organizational entity as required by this volume. (T-1)

(4) (Added)(AF) Assess reports concerning espionage, sabotage, subversive activities, deliberate compromises of classified information, and leaks of classified information to the media involving cleared facilities or visitor groups and determine appropriate risk-based countermeasures. (T-1) AFOSI is the investigating agency concerning these reports or any other similar actions.

d. (Added)(AF) The MAJCOM Director, Information Protection is responsible to the SPE for integrating the industrial security program into MAJCOM operations. (T-1) The MAJCOM IP Director will provide oversight and direction to the security specialists and other personnel assigned to the MAJCOM IP Directorate. (T-1) In addition to the requirements in AFI 16-1404 and DoDM 5200.02_AFMAN16-1405, the MAJCOM IP Director will:

(1) (Added)(AF) Assess requests for waivers, exceptions, or deviations to policy and validate the accuracy prior to endorsement by the SPE and submission to the appropriate organizational entity as required by this volume. (T-1)

(2) (Added)(AF) Inform the SPE of the security posture of contractor operations on Air Force installations. (T-1)

(3) (Added)(AF) Except under circumstances described in paragraph 8.2. of this volume, provide the SPE risk-based countermeasure strategies concerning reported espionage, sabotage, subversive activities, deliberate compromises of classified information, and leaks of classified information to the media involving cleared facilities or visitor groups located on or serviced by installations within the command. (T-1)

(4) (Added)(AF) Develop industrial security data calls or responses when requested. (T-1)

(5) (Added)(AF) Ensure supplemental industrial security policy is coordinated with

SAF/AAZ prior to publication in accordance with paragraph 2.7.b. of this volume. (T-1)

(6) (Added)(AF) Conduct required notifications in accordance with this volume when an on-installation cleared facility under the oversight of the command will receive a less than satisfactory rating during a security review or when an FCL under the oversight of the command will be invalidated or revoked. (T-1)

(7) (Added)(AF) Report security violations regarding on-installation cleared facilities as required by this volume. (T-1) Ensure up-to-date information regarding security violations is recorded in the SAF/AAZ designated repository. (T-1)

(8) (Added)(AF) Ensure security reviews are conducted for on-installation cleared facilities and required notifications are made in accordance with this volume. (T-1) Maintain up-to-date information regarding cleared facility profiles and security reviews in the SAF/AAZ designated repository. (T-1)

(9) (Added)(AF) Monitor less than satisfactory security reviews and invalidation or revocation proposals of cleared facilities under DCSA oversight until deficiencies are corrected or administrative action is taken to terminate the FCL. (T-1)

(10) (Added)(AF) Disseminate reports of contractor security violations received from DCSA to the appropriate GCA within the command. (T-1) Monitor the review of the security violation, ensure a classification review is conducted and the criteria for a damage assessment is evaluated, and a response is provided to the cognizant DCSA field office in accordance with this volume. (T-1) Ensure up-to-date information and documentation regarding these security violations are entered into the SAF/AAZ designated repository. (T-1)

e. (Added)(AF) The Installation Commander will oversee contractor operations requiring access to classified information while performing as a visitor or a cleared facility on the installation. (T-0) In addition to the requirements in AFI 16-1404 and DoDM 5200.02_AFMAN16-1405, the Installation Commander will:

(1) (Added)(AF) Submit to DCSA requests for waivers, exceptions, or deviations to policy regarding cleared facility oversight. (T-0) DCSA, as the CSO for cleared facilities, is the decision authority regarding requests for waivers, exceptions, or deviations to the National Industrial Security Program Operating Manual. The Installation Commander shall include a recommendation regarding the waiver, exception, or deviation to policy request in the staffing package and provide a copy to the MAJCOM Information Protection Office. (T-1)

(2) (Added)(AF) Grant contractors (e.g., prime contractors and subcontractors) access to the installation in accordance with AFMAN 31-113, *Installation Perimeter Access Control (FOUO)*. (T-1)

(3) (Added)(AF) Designate contractor operations requiring access to classified

information on the installation as cleared facilities, visitor groups, or intermittent visitors in accordance with this volume. (T-1)

(4) (Added)(AF) Upon designation of a contractor activity as a visitor group, ensure the contractor is provided a written copy of relevant local security policies (e.g., via email, electronic media, or paper) applicable to the contractor's on-installation access to classified information in support of the classified contract. (T-0)

(5) (Added)(AF) When designating an on-installation contractor operation as a cleared facility and retaining oversight of the cleared facility's security program, ensure sufficient resources are allocated to include industrial security, cybersecurity, and counterintelligence support in accordance with this volume. (T-0)

(6) (Added)(AF) Delegate oversight responsibilities in writing via support agreement, memorandum of understanding, etc., when another activity located on the installation (i.e., tenant organization's Information Protection Office) will provide oversight of on-installation cleared facilities or be responsible for processing and/or monitoring contractor visitor groups. (T-1)

f. (Added)(AF) Chief, Information Protection. The Chief, Information Protection should establish rapport with program or project managers, commanders/directors (hereinafter referred to as program/project managers), and the Director of Contracting for serviced organizations to ensure effective management of the industrial security program. The Chief, Information Protection will:

(1) (Added)(AF) Serve as the authority to perform industrial security program oversight for contractor operations on the installation and coordinate with DCSA when unique or special operational circumstances warrant and in all cases when the Air Force provides oversight of on-installation cleared facilities. (T-1) Maintain up-to-date information regarding cleared facility profiles and security reviews in the SAF/AAZ designated repository. (T-1)

(2) (Added)(AF) Except under circumstances described in paragraph 8.2. of this volume, brief the Installation Commander on reports concerning espionage; sabotage; subversive activities; deliberate compromises of classified information; and leaks of classified information to the media involving cleared facilities, visitor groups, or intermittent visitors and recommend appropriate risk-based countermeasures. (T-1)

(3) (Added)(AF) Develop staff packages to designate contractor operations as cleared facilities, visitor groups, or intermittent visitors. (T-1) This designation is determined by the visitor's relationship and interface with the AF activity and/or installation.

(4) (Added)(AF) Review reports of contractor security violations received through information protection channels or contracting channels from DCSA. (T-1) Ensure the appropriate GCA evaluates the report, conducts a classification review, evaluates the

criteria for a damage assessment, and a response is provided to the cognizant DCSA field office in accordance with this volume. (T-1) Maintain up-to-date information and documentation regarding these security violations in the SAF/AAZ designated repository. (T-1) If a damage assessment is required, refer to DoDM 5200.01 Volume 3, Enclosure 6 and AFI 16-1404, Chapters 3 and 7 for additional guidance. Provide notification to AFOSI if there is any suspicion of espionage, sabotage, subversive activities, deliberate compromises of classified information, and leaks. (T-1)

(5) (Added)(AF) Upon the Installation Commander's designation of a contractor activity as a visitor group, provide the contractor a written copy of relevant local security policies (e.g., via email, electronic media, or paper) applicable to the contractor's on-installation access to classified information in support of the classified contract. (T-1) Maintain a record of the communication in local industrial security files and destroy upon completion of on-installation performance as a visitor group. (T-1)

(6) (Added)(AF) When the Installation Commander has elected to retain security cognizance of on-installation cleared facilities, accomplish the following actions:

(a) (Added)(AF) Analyze and submit requests for waivers, exceptions, or deviations to policy regarding cleared facility oversight to the appropriate approval authority. (T-1)

(b) (Added)(AF) Make recommendations to the Installation Commander regarding proposed mitigation actions when security reviews of on-installation cleared facilities operating under the oversight of the Installation Commander result in less than satisfactory ratings. (T-1) Make notifications as required by this volume. (T-1) Record results in the SAF/AA designated repository. (T-1)

(c) (Added)(AF) Receive and evaluate security violation notifications from on-installation cleared facilities. (T-1) Make notifications in accordance with this volume. (T-1)

(d) (Added)(AF) Maintain and make notifications regarding on-installation FCL related documentation in accordance with this volume. (T-1) Maintain up-to-date information regarding cleared facility profiles and security reviews in the SAF/AAZ designated repository. (T-1)

(7) (Added)(AF) Review the DD Form 254 and Performance Work Statement, Statement of Work, or Statement of Objectives to ensure appropriate security language is incorporated into solicitations and contracts. (T-1)

(8) (Added)(AF) Report adverse information, suspicious contacts, security violations, espionage, sabotage, and subversive activities in accordance with this volume. (T-1)

(9) (Added)(AF) Provide or assist with locating industrial security training for

contracting officers, program managers, contracting officer representatives, and security assistants as appropriate. (T-1)

(10) (Added)(AF) Work closely with the host-installation cybersecurity office and local AFOSI detachment to ensure accomplishment of the requirements of this volume. (T-1)

(11) (Added)(AF) Administer account access to the National Industrial Security Program Contract Classification System (NCCS), the system used for DD Form 254 workflow, for individuals requiring a reviewer role (e.g., Information Protection Office, Special Security Officer, PSO, etc.) to perform security actions related to the DoD Activity Address Code (DoDAAC) corresponding with the cognizant contracting office(s). (T-1)

g. (Added)(AF) Contracting Officers. In accordance with the Federal Acquisition Regulation (FAR) Subpart 4.4 and associated supplements, the contracting officer is responsible for reviewing all proposed solicitations to determine whether access to classified information may be required by offerors or by a contractor during contract performance. (T-0) Contracting officers will require input and support from program managers, project managers, or other personnel knowledgeable of the contract requirements to perform this responsibility. Contracting officers will:

(1) (Added)(AF) If access to classified information is required during the solicitation phase or award phase of the contract, the contracting officer, in consultation with the program manager, shall:

(a) (Added)(AF) Include the appropriate security requirements clause from paragraph 52.204-2 of the FAR. (T-0) Include security safeguards in addition to those provided in the security requirements clause as appropriate when necessary to address unique security concerns. (T-0)

(b) (Added)(AF) Inform contractors and subcontractors of the security classifications and requirements assigned to the various documents, materials, tasks, subcontracts, and components of the classified contract. (T-0)

(c) (Added)(AF) Serve as the approving official for the DD Form 254 and ensure the DD Form 254 is prepared and distributed in accordance with this volume. (T-0) Particular attention should be taken to ensure the DD Form 254 is distributed 30 calendar days prior to classified work beginning to all government performance locations, normally to the installation Information Protection Office when performance is on an Air Force installation, to ensure the host Installation Commander is aware of the contractor's presence as a visitor on the installation. If the certified DD Form 254 cannot be provided to the installation Information Protection Office at least 30 calendar days in advance due to contract performance commencing in less than 30 calendar days from date of contract award, then the DD Form 254 is to be provided within 72 hours after contract award. (T-1) The contracting officer may designate an individual knowledgeable of the contract security requirements to prepare, approve, and distribute the DD Form 254 in accordance

with paragraph 3.4 of this volume. (T-1)

(2) (Added)(AF) Administer account access to NCCS for individuals requiring an initiator role (i.e., development of the DD Form 254), a certifier role (i.e., approving the DD Form 254 in block 17), or a contracting role (i.e., approve electronic dissemination of the DD Form 254 to the contractor) associated with the DoDAAC of the contracting office. (T-1)

(3) (Added)(AF) Upon receipt of notification of a contractor security violation from DCSA, the contracting officer or designee will ensure the owner of the classified information subject to loss, compromise, or suspected compromise (e.g., Original Classification Authority (OCA) or representative) is further notified and can perform required actions to mitigate potential damage in accordance with DoDM 5200.01 Volume 3, Enclosure 6 and AFI 16-1404, Chapters 3 and 7. (T-1)

h. (Added)(AF) System, Program, Project Managers, Commanders/Directors. These positions are referred to as program/project managers in this Air Force Manual. These positions are key to identification of specific types of information required by the contractor and provide security classification guidance by developing the DD Form 254. Program/project managers will:

(1) (Added)(AF) Prepare the DD Form 254 ensuring security requirements specific to the contract are included (T-1). Ensure coordination with other stakeholders is conducted as appropriate. (T-1)

(2) (Added)(AF) Identify contracts where access to proscribed information is required and prepare, coordinate, and submit requests for a National Interest Determination when a contractor operating under Foreign Ownership, Control, or Influence (FOCI) mitigated by a Special Security Agreement requires access to proscribed information to perform the requirements of the contract. (T-0)

(3) (Added)(AF) Review security violation reports and other products received from DCSA indicating classified information related to an Air Force contract is at risk of or has been the subject of loss, compromise, or suspected compromise. (T-0) Prepare a response to DCSA on behalf of the information owner (i.e., OCA) documenting the conduct of a classification review and a decision regarding whether a damage assessment was required in accordance with this volume. (T-1) Disseminate the response to DCSA through MAJCOM information protection channels. (T-1)

(4) (Added)(AF) Report changes through information protection channels to DCSA that could affect the FCL of a cleared contractor, including but not limited to: indicators of FOCI; federal law enforcement investigations of the company or its key management; debarment or exclusion of a cleared contractor; a company's request to terminate the FCL; etc. (T-0)

(5) (Added)(AF) Administer account access to NCCS for individuals requiring an

initiator role (i.e., development of the DD Form 254) or a reviewer role associated with classified contracts in support of the program/project office. (T-1)

SECTION 3: PROCEDURES

3.1. AMENDMENT OF VOLUME. Amendment of this volume, in accordance with DoDI 5220.22, requires coordination with the DoD Components and consultation with the non-DoD Components. Unless otherwise specified in any amendment, compliance with an amendment will not be mandatory until 30 days after date of publication, although compliance will be authorized from the date of its publication.

3.2. EXPENDITURE OF FUNDS FOR SECURITY. The CSO (be it DSS or the commander or head of a USG-controlled installation) will not commit the government to reimburse a contractor for funds expended in connection with the contractor's security program.

a. In the case of a cost-reimbursement-type contract, the allowability of security costs is determined by the contracting officer in accordance with the terms of the contract and with the cost principles of the Federal Acquisition Regulation (FAR). Under a fixed price contract, the initial contract price includes all applicable security costs. An equitable adjustment may be made in the initial contract price when, as indicated in the contract security clause, the security classification or security requirements under the contract are changed by the government (e.g., changes to DoD 5220.22-M, and the change results in an increase or decrease in contract price). DoD 5220.22-M provides that a U.S. contractor must implement changes no later than 6 months from the date of the published change to DoD 5220.22-M to allow the contractor to discuss what impact, if any, the changes have on existing classified contracts.

a. (Added)(AF) The contracting officer will evaluate changes to security requirements to determine any changes in contract scope, cost, or price in accordance with the FAR. (T-0)

b. As a precondition for receiving an FCL, DSS will require an uncleared company to execute the DD Form 441, "Department of Defense Security Agreement," located at http://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd0441_2017.pdf. When executing the DD Form 441, the uncleared company agrees to implement a security program meeting standards of DoD 5220.22-M and acknowledges that the agreement does not obligate government funds, nor does the government agree to any costs or claims of the contractor arising out of the agreement or its instructions.

3.3. EXCEPTIONS TO POLICY AND PROCEDURES.

a. The USD(I), or designee, will provide overall policy guidance to this program, in accordance with DoDI 5220.22 and will render decisions regarding exceptions to, or deviations from, the security policy and procedures promulgated in the volumes that comprise this manual. When required, the USD(I) or designee will coordinate with the applicable Component or its GCA and other elements of OSD having an interest in the matter. Exceptions will not be contrary to any existing Executive orders or laws. All requests for exceptions or deviations will include an explanation why the stated policy or procedures cannot be accommodated and a

proposed alternative with supporting justification, explaining how the alternative will result in substantially the same degree of protection. Requests will be submitted to OUSD(I) CI&S following the Component's procedures in accordance with Paragraph 3.4 of this volume. OUSD(I) CI&S will coordinate and consult on any requests for exception involving international security programs with the Office of the Under Secretary of Defense for Policy Director, International Security Programs, Defense Technology Security Administration, (referred to in this volume as "OUSD(P) Director, ISP").

a. (Added)(AF) Installation Commanders will submit requests for exceptions or deviations to the DoD requirements in this volume through MAJCOM information protection channels to SAF/AAZ. (T-1) SAF/AAZ will submit the requests to the Office of the Under Secretary of Defense for Intelligence (OUSD(I)). (T-1)

b. Any conflict that develops between instructions in the volumes of this manual will be reported to OUSD(I) CI&S following Component procedures in accordance with Paragraph 3.4 of this volume. Pending resolution, the provisions of this volume will govern.

3.4. COMPONENTS AND THEIR GCAS.

a. The Component will require their GCAs to provide an executed DD Form 254 or security aspects letter, if applicable, as an attachment to contracts, solicitations, and other arrangements or agreements that require access to classified information. The DD Form 254 or security aspects letter, if applicable, should be provided to affected contractors, to the applicable GCA elements as defined in Component procedures and to the responsible DSS field activities. The DD Form 254 and its associated instructions are located at http://www.esd.whs.mil/portals/54/documents/dd/forms/dd/dd0254.pdf and http://www.esd.whs.mil/portals/54/documents/dd/forms/dd/dd0254-Inst.pdf, respectively.

(1) (Added)(AF) In accordance with the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) memorandum, *Use of the National Industrial Security Program Contract Classification System*, dated February 8, 2018 and the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) memorandum, *Use of National Industrial Security Program Contract Classification System*, dated October 19, 2018, Air Force personnel will use NCCS to automate DD Form 254 processes and workflows where possible. (T-0) NCCS is available electronically at the Procurement Integrated Enterprise Environment (PIEE) system at https://wawf.eb.mil. Information Protection Offices will manage NCCS accounts for security-related personnel requiring a reviewer role. (T-1) Personnel representing the acquisition/contracting/program management functional areas will manage NCCS accounts for personnel requiring an initiator, certifier, contracting, or reviewer role unrelated to the security review. (T-3) For contracts where the content of the DD Form 254 contains classified information and the classified information cannot be segregated into classified attachments or addendums, use of NCCS is not required until such time that an automated solution is available on the appropriate classified information system.

(2) (Added)(AF) In the absence of exceptional circumstances that clearly support

classification, the DD Form 254 will not be classified. If classified supplements are required as part of the contract security classification specification, the contracting officer must ensure they are identified in block 13 of the DD Form 254 and furnished as an attachment or forwarded to the contractor by separate correspondence. (T-0)

(3) (Added)(AF) Contracting officers, in coordination with program management (e.g., requirements owner), will ensure the contents of the DD Form 254 are complete and adequate for safeguarding the classified information to be released or generated under the classified effort. (T-0) The contracting officer may designate an individual knowledgeable of the requirements of the contract (e.g., program manager, contracting officer's representative, etc.) to serve as the certifying official of the DD Form 254 and sign in block 17. The contracting officer will prepare the designation in writing with copies maintained by the contracting officer and the designee, and ensure it is available for review during self-inspections and other oversight activities. (T-1) The designation must include the following:

(a) (Added)(AF) The contracting officer and the designee must both sign the designation letter to document the authority for the designation and the acceptance of responsibility. (T-1)

(b) (Added)(AF) The contracting officer will ensure the designation letter includes a statement that the designee is knowledgeable of the requirements of the contract, an acknowledgement that the DD Form 254 must be coordinated with program management and security officials based on the contract requirements, has reviewed the DD Form 254 Instructions, *Instructions for Completing DD Form 254, Department of Defense Contract Security Classification Specification* available at the DoD Directives website at https://www.esd.whs.mil/DD, and is aware of their responsibilities under the Federal Acquisition Regulation and its supplements. (T-1)

(c) (Added)(AF) The designee shall be a government employee (civilian or military). (T-0) Contractor employees will not serve as certifiers of DD Forms 254 through designation by a contracting officer. (T-0)

(d) (Added)(AF) The contracting officer will ensure the DD Form 254 is prepared and distributed in accordance with the Federal Acquisition Regulation, Subpart 4.4. and this volume. (T-0)

(4) (Added)(AF) Contracting officers or designees will ensure the DD Form 254 is coordinated with the offices in 3.4.a.(4)(a) through 3.4.a.(4)(d) prior to certification, and the coordination will be documented in writing or electronically in NCCS. (T-1)

(a) (Added)(AF) Contracting officers will ensure the DD Form 254 is reviewed by the servicing Information Protection Office in all cases other than circumstances when the DD Form 254 contains SAP information not reviewable by the Information Protection Office. (T-1)

(b) (Added)(AF) When block 10(e) of the DD Form 254 is selected, coordinate with the servicing Special Security Officer (or designee). (T-1)

(c) (Added)(AF) When block 10(f) of the DD Form 254 is selected, coordinate with the servicing PSO or designee and, when required, Government SAP Security Officer. (T-0)

(d) (Added)(AF) Contract security requirements are to be coordinated with program management (e.g., requirements owners) and incorporated into contract documentation (e.g., Performance Work Statement, Statement of Work, Statement of Objectives) to reflect the requirements annotated on the DD Form 254. (T-1)

(5) (Added)(AF) When preparing the DD Form 254, ensure the "Through" block is selected in block 12 Public Release and the following statement is included: "Contractor is to submit requests through the contracting officer for OPSEC program manager review and public release authorization. The contracting officer will provide contractor with written approval/disapproval. Information requiring AF or DoD-level review will be reviewed by the unit's OPSEC program manager or coordinator who will in-turn forward to the entry-level public affairs office through the AFIMSC Public Affairs Office to the Secretary of the Air Force, Office of Public Affairs, Security and Review Division (SAF/PAX), 1690 Air Force Pentagon, Washington DC 20330-1690." MAJCOM/DRUs will send information requiring AF or DoD-level review directly to SAF/PAX. (T-1)

(6) (Added)(AF) The contracting officer or designee will identify by title, functional OPR, and approval date (to include letter changes) the specific security classification guidance or guides applicable to the contract in block 13 of the DD Form 254 in accordance with Paragraph 6.3.d. of this volume. (T-1) If the title to the guidance is classified, it may be provided in a classified supplement or attachment.

(7) (Added)(AF) At a minimum, the contracting officer or designee will ensure the DD Form 254 is distributed as follows in accordance with the Federal Acquisition Regulation and supplements. (T-0) Program managers will provide the contracting officer a list of additional distribution requirements beyond those identified in Paragraphs 3.4.a.(7)(a) and 3.4.a.(7)(b) below. (T-1)

(a) (Added)(AF) Distribute a copy of the DD Form 254 to the contractor as a part of the official contract. (T-0)

(b) (Added)(AF) Distribute a copy of the DD Form 254 to the CSO(s) identified in blocks 6, 7, and 8. (T-0) When the contract requires performance on a military installation or multiple installations, distribute a copy of the DD Form 254 to the host Information Protection Office (or Army, Navy, Marine Corps, Coast Guard equivalent) where performance will occur at least 30 calendar days prior to the start of contract performance. (T-1) If the certified DD Form 254 cannot be provided to the installation Information Protection Office at least calendar 30 days in advance due to contract performance commencing in less than calendar 30 days from date of contract award, then

the DD Form 254 is to be provided within 72 hours after contract award. (T-1)

(8) (Added)(AF) Air Force personnel will use the DD Form 254 Instructions available at the DoD Directives website at https://www.esd.whs.mil/DD for instructions on how to correctly prepare the DD Form 254. (T-1) This document provides detailed information on factors to consider when incorporating security requirements into the contract, provides context for each field in the DD Form 254, and serves as policy for the correct preparation of the DD Form 254.

b. If the Component or GCA chooses to augment this volume with any detailed procedures, the Component will ensure that those procedures are consistent with the provisions of this volume. The Component or GCA detailed operating procedures will also be consistent with the requirements, restrictions, and safeguards that directives implementing ICD 700 or Section 2011 et seq., of Title 42, U.S.C. (also known and referred to in this volume as "The Atomic Energy Act of 1954, as amended") establish for the protection of classified information by GCAs.

3.5 SECURITY COGNIZANCE WITHIN THE UNITED STATES, ITS TERRITORIAL AREAS, AND THE DISTRICT OF COLUMBIA. Overall security cognizance for each contractor facility will be provided by only one of the five NISP CSAs in the case of contractors with contracts requiring access to classified information from more than one CSA (i.e., DoD, DOE, Office of the Director of National Intelligence, Nuclear Regulatory Commission, or DHS). When DoD and another NISP CSA have classified involvement at the same contractor facility, DSS, as the CSO, will determine security cognizance, in coordination with the other CSA. That determination will be made consistent with the provisions of Part 2004 of Title 32 CFR based upon the preponderance of classified involvement (e.g., the highest level of classified performance or volume of classified work as the number of classified contracts need not be the sole, determining factor) and will include execution of a memorandum of agreement between DSS and the other NISP CSA relating to each affected contractor. DSS will then notify all affected Components for which DSS serves as the CSO whether DSS or another CSA has security cognizance.

a. DSS, when acting as the CSO:

(1) Exercises security cognizance, in accordance with this manual, for any U.S. company with an FCL (otherwise referred to in this manual as a U.S. contractor) in the United States, the District of Columbia, and its territories (see Paragraph 4.4.b of this volume). Such cognizance does not include those FCLs on USG-controlled installations where the commander or head of the USG installation (referred to in this volume as "Commander")) has retained security cognizance pursuant to Paragraph 3.8.c of this volume.

(1) (Added)(AF) In circumstances where the Installation Commander retains security cognizance of cleared contractor facilities on the installation, DCSA retains CSO authorities and responsibilities while the Installation Commander retains oversight responsibilities in accordance with Paragraph 3.8. of this volume.

(2) Assigns security cognizance to a DSS region or field office and post a list of the region or field offices and their assigned areas of responsibility at www.dss.mil.

(3) Advises the uncleared company during the initial facility clearance process which DSS office has security cognizance.

(4) Provides the Commander with the contact information for the applicable DSS office that serves as a liaison to the Commander for any FCLs on a USG-controlled installation. Security cognizance and oversight of contractor operations located on a USG-controlled installation are addressed in paragraph 3.8 of this volume.

b. A representative of a GCA will notify DSS, as the CSO, of any GCA visits to a contractor to review security aspects of a collateral contract requiring access to classified information or FGI. Any significant deviation from the requirements of DoD 5220.22-M that may be noted during the visit will be referred promptly to DSS, along with any suggested corrective action or additional security requirements to be levied on the contractor. DSS will be responsible for ensuring appropriate action is taken regarding these matters, and will notify the GCA of the corrective action taken by the contractor.

b. (Added)(AF) This paragraph applies when DCSA provides security oversight of the cleared contractor facility and does not apply in cases where the Installation Commander retains oversight of cleared contractor facilities on the installation.

3.6. SECURITY COGNIZANCE FOR SAPS WITH CONTRACTORS. Security cognizance with respect to the DoD and industry contracts involving DoD SAPs is stipulated in this section and in accordance with E.O. 13526 and DoDD 5205.07. The security measures for SAPs that are in addition to those prescribed in DoD 5220.22-M for collateral contracts are contained in Appendix D of DoD 5220.22-M, and the DoD Special Access Program (SAP) Security Manual, Volumes 1-4.

a. The Director, DSS, or upon delegation, the DSS Regional Directors, will exercise security oversight for DoD SAPs operating consistent with the NISP and perform the following security functions to satisfy SAP requirements:

(1) Exercise security oversight in accordance with the provisions of this manual. DSS will record the highest classification level eligible, however, DSS will not record or verify contractor eligibility for access or possession of SAP information.

(2) Provide the SAP GCA written reports conveying security review results, as well as the security posture of the contractor and any threat or incident information that relates specific threats to the technology or geographic area of interest. When appropriate, any such threat and incident information will also be provided to the contractor’s security personnel and GCA counterintelligence (CI) support personnel.

(3) Notify the SAP GCA of security issues that may affect SAP information in the hands of a contractor.

b. When DSS is the CSO, GCAs:

(1) Notify DSS of the applicable GCA SAP security officers and provide updates as necessary for SAPs that have DSS security cognizance.

(2) Ensure that any adverse information coming to the attention of the GCA regarding a contractor employee whose clearance is maintained by the DoD is provided to DSS.

c. When the SecDef or the Deputy Secretary of Defense determine that the security interests of DoD and the sensitivities of a SAP warrant, he or she may relieve DSS of this oversight responsibility and assign security cognizance to another DoD Component. When this occurs, the contracts are referred to as "carve-outs." Generally, this mechanism is used when knowledge of the existence of a particular contract or its association with the SAP is classified and designated as SAP protected information. In these instances, the DoD Component that assumes security cognizance will:

(1) Advise the DoD Special Access Program Central Office (SAPCO) of the creation and continuing existence of the carve-out to ensure the DoD SAPCO is aware of this arrangement should relevant security changes arise; e.g., the prospective acquisition of the contractor by a foreign interest. The DoD SAPCO will implement a mechanism to facilitate DSS awareness of approved carve-out arrangements at contractors.

(2) Perform all security oversight functions for the applicable SAP in accordance with the provisions of this manual and reflect the carve-out status of a contract on the DD Form 254.

d. (Added)(AF) The Air Force assumes security cognizance of SAP contracts where contractor performance takes place within a SAP Facility. PSOs will coordinate with the appropriate contracting officer and program manager to validate DD Forms 254 contain language indicating DCSA and/or Air Force Information Protection Offices are "carved out" of program oversight and identify the Air Force Office of Special Investigations, Office of Special Projects (AFOSI PJ) as having security oversight and compliance inspection responsibility. (T-1) DCSA will continue to serve as the CSO for the FCL. For on-base performance, the servicing Information Protection Office will provide oversight of any collateral performance outside a SAP Facility but will provide no oversight of the space (e.g., oversight of collateral classified material or Controlled Unclassified Information contained therein). (T-1) For contracts with SAP access, a DD Form 254 may be certified only after endorsement by a program manager and PSO. Contracting officers may designate certification of the DD Form 254 in accordance with paragraph 3.4.a.(3). The cognizant PSO will provide oversight of SAP material and spaces in in contractor facilities in accordance with AFI 16-701, *Management, Administration and Oversight of Special Access Programs*.

3.7. SECURITY COGNIZANCE FOR THE PROTECTION OF SCI WITH CONTRACTORS.

a. Oversight of the protection of SCI in the hands of contractors is the responsibility of the

GCA in accordance with Section 3024 of Title 50, U.S.C. as implemented in ICD 700. SCI released to contractor personnel will be controlled in accordance with the provisions of Director of Central Intelligence Directive 6/1, DoDM 5105.21, Volumes 1-3, and implementing Component policies.

a. (Added)(AF) Air Force contracts that include requirements for access to SCI typically "carve out" DCSA and/or Air Force Information Protection Offices from oversight of the information as well as spaces where SCI is stored. DCSA will continue to serve as the CSO for the FCL and for on base performance, the servicing Information Protection Office will provide oversight of any collateral performance outside an SCI Facility but will not provide oversight of the space where SCI is stored to include any non-SCI material stored in the space (e.g., collateral classified material, Controlled Unclassified Information, etc.). The cognizant Special Security Officer Responsibility will provide oversight of SCI material and spaces at contractor facilities in accordance with AFI 14-403, *Sensitive Compartmented Information, Security and Intelligence, Surveillance, and Reconnaissance Systems Cybersecurity and Governance*.

b. Before releasing or providing SCI to contractor personnel, the GCA will ensure that they are appropriately cleared in accordance with ICD 704 and they agree to follow controls and procedures for the protection, handling, and accountability of SCI. All activities involving SCI (including discussions) will be conducted in sensitive compartmented information facilities (SCIFs). Physical security standards for SCIFs are contained in ICD 705, applicable IC specifications, or standards and implementing DoD Component policies.

c. While DSS has no responsibility for the oversight of the protection of SCI, the Director, DSS, or designee:

(1) Maintains FCLs for contractors working on contracts involving access to, or possession of, SCI, when requested by an SCI CSO. DSS will not record or verify contractor eligibility for access to or possession of SCI or SAP information.

(2) Provides the SCI CSO written reports conveying security review results, as well as the security posture of the contractor and any threat or incident information that relates specific threats to the technology or geographic area of interest. When appropriate, provides such threat and incident information to the contractor's security personnel.

(3) Notifies the SCI CSO of security issues that may affect the protection of SCI information in the hands of a contractor.

(4) Notifies an SCI CSO if it becomes aware of a contractor storing collateral classified information not specific to the GCA programs within the SCI CSO accredited space without prior written approval from the approving SCI CSO and the supported GCAs.

(5) Coordinates with the Office of the National Counterintelligence and Security Center with regard to evaluation and approval of access to SCI by foreign-owned U.S. cleared companies or any other Intelligence Community equities in accordance with the provisions of

Volume 3 of DoDM 5220.22 and also Directive-type Memorandum 15-002 to provide updated guidance.

(5) (Added)(AF) When an Air Force contract requires SAP access in addition to access to SCI, SAF/AAZ coordinates with the Office of the National Counterintelligence and Security Center to request approval of access to SCI by foreign-owned U.S. cleared companies in accordance with DoDM 5220.22, Volume 3. (T-1) DCSA is carved out of this process in cases when the Air Force contract also includes a requirement for access to SAP information.

d. An SCI CSO and the GCAs within an SCI CSO accredited space must provide prior written approval for storage of collateral classified information not specific to the GCA programs within the applicable SCI CSO accredited space. Based upon that written approval, DSS would not have oversight responsibility for such collateral classified information in the applicable SCI CSO accredited space. The SCI CSO would have oversight of that collateral classified information even though it is not specific to the GCA programs within the applicable SCI CSO accredited space because of the written approval for storage.

3.8. CONTRACTOR OPERATIONS ON USG CONTROLLED INSTALLATIONS. A contractor's personnel assigned to a USG-controlled installation to perform operations that require access to classified information for the Commander or a GCA may be considered visitors, notwithstanding the duration of the assignment, and are subject to the security procedures of the installation and as applicable, a tenant command. Alternatively, the Commander may request an FCL subject to the provisions of Paragraph 3.8.b of this volume and Section 4 of this volume.

a. Visitors to a USG-Controlled Installation. The Commander or designee will provide security oversight of all contractor visitors, in which case, they will follow the security procedures of the installation. When requested by the Commander, any GCA-controlled location on the installation will execute an agreement with the host installation setting forth the security procedures that contractor visitors will be required to follow.

a. (Added)(AF) The contracting officer, as part of the process of coordinating the DD Form 254 with internal Air Force organizations, will ensure instructions regarding the protection of classified information on the installation are included with the DD Form 254. (T-0) If the protection requirements are too lengthy to be provided with the DD Form 254 due to on-installation performance at multiple government locations, the location specific instructions may be provided to the contractor under the visitor group procedures identified in this volume.

(1) (Added)(AF) The contracting officer, or designee, will ensure dissemination of the DD Form 254 to the Chief, Information Protection at all Air Force installations identified as performance locations at least 30 calendar days prior to the start of contract performance. (T-1) If performance is on other military service installations, the contracting officer, or designee, will follow the other service's or installation's requirements for dissemination of the DD Form 254. (T-1)

(2) (Added)(AF) Upon notification of the presence of a visitor group, the Chief, Information Protection is responsible for communicating the local security policies where classified performance will occur to the contractor in writing (e.g., email, electronic media, or paper) and retaining documentation of the communication in local industrial security files until contract termination. (T-1)

(3) Installation Commanders will categorize on-site contractors as visitor groups, intermittent visitors, or cleared facilities. (T-1)

(4) Contractors that cannot be categorized as cleared facilities or visitor groups will be categorized as intermittent visitors. Contractor operations performing less than 90 calendar days qualify as intermittent visitors. Intermittent visitors may operate under the security requirements of DoD 5220.22-M or the installation security program. Generally, contractor operations of 90 calendar days or more are designated visitor groups. If within the scope of the contract, contractors categorized as visitor groups are permitted to conduct end of day checks, have access to GSA approved security containers, and/or have access to applicable alarm codes for secure areas. Visitor groups may operate in two different ways, both under the policy guidance of this volume and AFI 16-1404. Visitor groups can:

(a) (Added)(AF) Operate under day-to-day oversight of an Air Force activity. In these cases, the Commander/Director will integrate contractor employees into their Information Security Program. These contractor employees typically sit in the same work-space as government employees where an Air Force official is responsible for the security requirements of the space. Contractors who operate as an integrated visitor group remain subject to this volume and AFI 16-1404 and must provide an on-site Security Point of Contact to the Information Protection Office as required by contract.

(b) (Added)(AF) Operate independently from an on-base Air Force activity. In these cases, the contractor employees operate independently from day-to-day oversight by Air Force employees and typically have a separately assigned space for which they are responsible as described in memoranda of agreement, support agreements, etc. Further, contractors are normally only categorized this way when their contract requires them to store classified information and they do so separately from other Air Force operations. Contractors who operate as an independent visitor group remain subject to this volume and AFI 16-1404 and must identify an on-site Security Point of Contact to the Information Protection Office as required by contract. The Security Point of Contact will ensure the required security responsibilities of the contractor are performed.

b. FCLs on a USG-Controlled Installation. DSS may process a contractor's operation on any USG-controlled installation for an FCL if the contractor is otherwise eligible for an FCL in accordance with Section 4 of this volume and all of the following criteria apply:

b. (Added)(AF) The initial determination regarding whether a contractor's operation on an Air Force controlled installation should be categorized as a cleared facility rests

with the Installation Commander. Installation Commanders will coordinate requests for new on-installation cleared facilities through MAJCOM information protection channels prior to submission to DCSA. (T-1) DCSA will review the request from the Installation Commander, validate the fulfillment of the requirements identified in paragraphs 3.8.b.(1) through 3.8.b.(5) of this volume, and process actions to establish the cleared facility. In lieu of a cleared facility, the Installation Commander may determine to manage the contractor's on-installation performance as a visitor.

(1) The contractor's operation is sufficiently complex to warrant assignment of a segregated work area such as a suite of offices, a building, or portion thereof.

(2) The contractor maintains a long-term operational presence on the installation (i.e., of a year or more).

(3) The contractor maintains management control over its operations.

(4) The contractor is in a position to maintain security procedures that are separate from the host activity and in accordance with the terms of any formal agreement with the tenant DoD Component or host installation and DoD 5220.22-M.

(5) If located on a USG-controlled installation in a foreign country, the contractor is a branch or division office of an already cleared U.S. contractor in the United States, or of a U.S. company being processed for an FCL in the United States.

c. Security Cognizance of a Cleared Facility on a USG-Controlled Installation

(1) If the Commander decides that a contractor's on-installation operations requires an FCL and meets the provisions of Paragraph 3.8.b of this volume, the Commander will ordinarily request DSS to assume security cognizance in accordance with Section 4 of this volume. If DSS assumes security cognizance, DSS is responsible for all aspects of security oversight, except if the proposed FCL will be located on a USG-controlled installation in a foreign country. In such cases, before an FCL will be granted, DSS and the Commander must establish a formal agreement that sets forth how oversight will be conducted because DSS may require assistance for aspects of the oversight from the Commander or sponsoring tenant USG activity depending upon the location.

(1) (Added)(AF) Commanders of Air Force installations in foreign countries will provide a copy of the formal agreement between the Installation Commander and DCSA through MAJCOM information protection channels to SAF/AAZ. (T-1) Coordination with SAF/AAZ prior to signing and submitting the formal agreement to DCSA is recommended to ensure the request addresses all required responsibilities.

(2) If a tenant USG activity decides that a contractor's on-installation operation requires an FCL, and meets the provisions of Paragraph 3.8.b of this volume, the tenant USG activity may submit a request for FCL through the Commander. The Commander may:

(a) Endorse the FCL sponsorship request and submit it to DSS.

(b) Disapprove the request and handle the contractor's operation as a visitor group. The Commander is responsible for all aspects of security oversight.

(c) Retain security cognizance for the sponsored FCL. If the Commander has compelling reasons, as described in Paragraph 3.8.c.(5) of this volume, to retain security cognizance and so formally advises DSS, the Commander is responsible for all aspects of security oversight.

(3) Responsibility will not be divided between the Commander and DSS unless the provisions of Paragraph 3.8.c.(1) of this volume apply where the proposed FCL will be located on a USG-controlled installation in a foreign country.

(3) (Added)(AF) When the Installation Commander assumes oversight responsibility for an on-installation cleared facility, the Commander must provide industrial security support to include authorizing and providing oversight for classified information systems operating within the facility and providing counterintelligence support in accordance with this volume. (T-0) The ability to provide such support should be considered when evaluating whether DCSA or the Commander is best suited to provide security oversight of the contractor facility. When DCSA retains security cognizance of an on-installation cleared facility, classified information systems operating under Air Force authorizations may potentially be introduced into the facility under Federal Information System procedures upon agreement by DCSA. Procedures for requesting introduction of a Federal Information System into a facility under DCSA security cognizance are identified in the *DSS Assessment and Authorization Process Manual (DAAPM)* located on DCSA's website at www.dss.mil.

(4) DSS will annually provide a list of all on-base cleared facilities to the designated industrial security point of contact for each of the Military Services, noting whether DSS or a Commander retains security cognizance. If DSS has security cognizance of a cleared facility on a USG-controlled installation, DSS will:

(4) (Added)(AF) SAF/AAZ, serving as the designated industrial security point of contact for the Air Force, will share the list of all on-base cleared facilities with Installation Commanders through information protection channels to validate the information contained therein. (T-1)

(a) Exercise security oversight of the contractor facility in accordance with the provisions of this manual.

(b) Notify the Commander of any significant changes at the contractor as such changes occur.

(c) Provide the Commander with copies of all suspicious contact reports submitted.

(d) Notify the Commander immediately if any security review rating is marginal or unsatisfactory as described in Section 14 of this volume and provide the Commander with an update after completion of any compliance security reviews.

(e) Provide the Commander copies of any reports resulting from investigations conducted in cases of loss, compromise, or suspected compromise of classified information.

(5) If the Commander decides to retain security cognizance, the Commander will notify DSS in writing, explaining why the contractor operations are of such criticality to the installation mission (e.g., the company's work is essential to the safety or security of the installation or the classified program is at a high level of sensitivity, such as a SAP) that retention of security cognizance is necessary. The Commander will also include the compelling reasons to retain security cognizance in any new FCL sponsorship letters to DSS. DSS will not process the new FCL until security cognizance responsibility is resolved.

(5) (Added)(AF) Installation Commanders will provide a copy of the request to DCSA to retain security cognizance of the cleared facility through MAJCOM information protection channels to SAF/AAZ. (T-1) Coordination with SAF/AAZ prior to signing and submitting the request to DCSA is recommended to ensure the request is thorough and complete. In addition to including the compelling reasons to retain security cognizance, Installation Commanders will include a statement expressing commitment to sufficiently resource the oversight responsibilities. (T-1) Prior to accepting oversight responsibility for an on-installation cleared facility, the Installation Commander must coordinate with SAF/IGX to ensure Air Force Office of Special Investigation resources are available to support the counterintelligence oversight requirements of this volume. (T-1)

(a) If the Commander retains security cognizance, the Commander will:

1. Request that DSS process the company for an FCL, (including adjudication of foreign ownership, control, or influence (FOCI) factors, if applicable) based on a legitimate government requirement for access to classified information in accordance with Section 4 of this volume.

2. Provide security oversight of the contractor by personnel trained in accordance with Paragraph 2.7.c of this volume and the provisions of this manual.

2. (Added)(AF) When the Installation Commander assumes oversight responsibility for the cleared facility, the Commander must provide sufficient security oversight support to ensure the contractor executes its industrial security responsibilities in accordance with DoD 5220.22-M and this volume. (T-0) Security oversight support includes but is not limited to processing approvals of classified processing areas and closed areas, conducting security reviews of contractor security operations, providing counterintelligence services and oversight, and authorizing and providing oversight for classified information systems operating within on-installation contractor cleared facilities. When the Commander determines there are no longer adequate resources to provide security oversight or conditions have changed such that a request to transfer

oversight responsibility to DCSA is considered, a request will be made to DCSA to transfer security oversight responsibilities to DCSA. (T-0) Commanders will submit these requests through MAJCOM information protection channels. (T-1)

3. Notify DSS of any changes affecting the FCL (e.g., change of ownership, change of management personnel, change in FOCI factors, change in safeguarding capability, or any other factors in DoD 5220.22-M).

4. Approve safeguarding capability, if needed to perform on a classified procurement requirement and provide notice to DSS of the initial approval and immediate notice of any changes to that safeguarding capability.

4. (Added)(AF) Air Force Information Protection Offices will review and approve safeguarding capability for on-installation cleared facilities in accordance with the safeguarding requirements identified in DoD 5220.22-M. (T-1)

5. Require that the contractor report promptly to the Commander and to DSS any suspicious contacts and any incidents which involve actual, probable or possible espionage, sabotage, terrorism, or subversive activity, or the loss, compromise, or suspected compromise of classified information in accordance with DoD 5220.22-M.

6. Notify DSS immediately if any security review rating is marginal or unsatisfactory as described in Section 14 of this volume and provide DSS with an update regarding the security review rating after completion of any compliance security reviews.

6. (Added)(AF) Installation Commanders will provide notification to DCSA regarding marginal or unsatisfactory security review ratings through SAF/AAZ through MAJCOM information protection channels. (T-1)

7. Provide an annual certification to DSS that the cleared facility is still able to properly protect classified information, on or about the anniversary date of the FCL, based on the Commander's recurring security reviews. This annual certification from the Commander will serve as the basis for DSS to continue to verify the FCL and, as applicable, the safeguarding capability of the cleared facility. The annual certification will include, but is not limited to:

7. (Added)(AF) Installation Commanders will provide a copy of the annual certification to SAF/AAZ through MAJCOM information protection channels. (T-1)

a. Dates and ratings of record for security reviews conducted since the last annual certification.

b. The most recent list of key management personnel (KMP).

c. The current FCL level and approved safeguarding level.

d. An update on any FOCI changes to the contractor.

8. Recommend to DSS the termination, invalidation, or revocation of the FCL, when warranted.

8. (Added)(AF) Installation Commanders will provide a copy of requests to terminate, invalidate, revoke, or transfer oversight responsibilities for the FCL to SAF/AAZ through MAJCOM information protection channels. (T-1)

(6) When the Commander retains security cognizance over a contractor with an FCL, the DSS will:

(a) Grant the FCL to the company which includes adjudication of existing FOCI factors, if applicable, in accordance with the provisions of this manual.

(b) Terminate, invalidate, or revoke the FCL, as appropriate, in accordance with procedures in Section 4 of this volume and notify the GCA.

(7) (Added)(AF) Installation Commanders will provide copies of all documentation related to requests for FCLs and termination of FCLs on USG-Controlled Installations through MAJCOM information protection channels to SAF/AAZ at each stage of the FCL-establishment/disestablishment process. (T-1) SAF/AAZ uses the information provided to ensure the requirement of Appendix 4A and Section 14 of this volume are provided to DCSA, to inform SAF/AA as the Senior Agency Official for Security of the state of cleared facilities across the Air Force security enterprise, and to provide oversight of the on-installation cleared facility requirements established by this volume.

3.9 REPORTING REQUIREMENTS TO ISOO.

a. DoD Components will promptly report violations, described in Paragraphs 3.9.a.(1) and 3.9.a.(2) of this volume, to the OUSD(I) CI&S, which will, in turn, submit a report to the Director, ISOO, consistent with DoD 5220.22-M and pursuant to parts 2001 and 2004 of Title 32 CFR. Parts 2001 and 2004 of Title 32 CFR require agency heads or senior agency officials to provide such reporting, when officers and employees of the USG and its contractors, licensees, certificate holders, and grantees knowingly, willfully, or negligently:

a. (Added)(AF) Installation Commanders will report the violations listed in Paragraphs 3.9.a.(1) and 3.9.a.(2) in accordance with the procedures identified in AFI 16-1404. (T-1)

(1) Create or continue a SAP contrary to the requirements of E.O. 13526.

(2) Disclose to unauthorized persons information properly classified pursuant to E.O. 13526 or predecessor orders or classify or continue the classification of information in violation of E.O. 13526 or its implementing directives that:

(a) Is reported to oversight committees in the Legislative Branch;

(b) May attract significant public attention;

(c) Involves large amounts of classified information; or

(d) Reveals a potential systemic weakness in classification, safeguarding, or declassification policy or practices.

b. In accordance with E.O. 13526 and pursuant to Parts 2001 and 2004 of Title 32 CFR, the Director, DSS:

(1) Conducts an annual analysis of contractor costs associated with implementing the NISP.

(2) Provides the cost analysis to the Director, ISOO, with a copy to the OUSD(I) CI&S annually.

(3) Maintains the underlying cost collection methodology and cost collection analysis.

3.10. HANDLING INFORMATION REPORTED BY OR ABOUT CONTRACTORS.

a. General. DSS or the DoD Consolidated Adjudications Facility (DoD CAF) will review reports, as applicable, submitted in accordance with DoD 5220.22-M on contractors or individuals (e.g., adverse information, probable or possible espionage, sabotage, suspicious contacts, loss, compromise or suspected compromise, individual culpability) to assess the impact on the facility clearance or personnel security clearance and take appropriate action. See Sections 4, 5, and 8 of this volume for additional guidance.

b. Information Reported About Contractors. Such reports, other than those already classified or appropriately marked, will be marked "FOR OFFICIAL USE ONLY" or FOUO upon receipt. For additional guidance, refer to Volume 4 of DoDM 5200.01. When requests for such records are made pursuant to Section 552 of Title 5, U.S.C. (also known as the "Freedom of Information Act, as amended) DSS or the DoD CAF will determine whether to invoke applicable exemptions under those statues to withhold the reported information from disclosure.

b. (Added)(AF) When reports are submitted to Air Force officials (e.g., Information Protection Office, program manager, contracting officer, etc.) in accordance with DoD 5220.22-M regarding contractors or individuals as described in paragraph 3.10.a., the Air Force recipient of the information will ensure any written or electronic products containing the information are marked as described in this paragraph. (T-0) Additionally, the Air Force will determine whether to invoke the exemptions identified in this paragraph to withhold the reported information from disclosure in accordance with DoDM 5400.07_AFMAN33-302, *Freedom of Information Act Program*.

c. Information Reported About Individuals. DSS will manage and safeguard reports submitted or information provided about an individual in accordance with DoDD 5400.11, and DoD 5400.11-R.

c. (Added)(AF) The Air Force will manage and safeguard reports submitted or information provided about an individual in accordance with AFI 33-332, *Air Force Privacy and Civil Liberties Program*.

(1) When such reports contain information pertaining to an individual, that information may be provided to the individual, except for information for which an exemption is available and asserted pursuant to Section 552 of Title 5, U.S.C. (For guidance on applying exemptions under the Privacy Act and FOIA, refer to Section 3.9 of DoDM 54007.07, DoD Freedom of Information Act (FOIA) Program). This may include the identity of a source who has furnished information to the government based on an expressed promise of confidentiality.

(2) Should action for defamation of character be brought against a contractor or its employees for reporting information concerning an individual in accordance with the requirements of DoD 5220.22-M, and the defendants in the suit seek the assistance of the DoD in defending against the suits, their request should be referred to OUSD(I) CI&S for appropriate action.

3.11. ISLS.

a. DSS, with the concurrence of USD(I), issues ISLs as needed to provide clarification, interpretation, and guidance to contractors in carrying out their responsibilities consistent with the NISP and to provide other security-related implementation guidelines in accordance with DoDI 5220.22.

a. (Added)(AF) When providing oversight of on-installation cleared facilities, Information Protection Offices and other oversight activities (i.e., Cybersecurity Squadrons and AFOSI detachments) will use DCSA Industrial Security Letters to apply interpretations of the requirements of DoD 5220.22-M to the oversight of the cleared facilities. (T-1)

b. Components as well as their GCAs, OSD elements and contractors may submit proposed articles for issuance in ISLs to DSS.

c. ISLs that deal with the ITAR security requirements, the international security requirements of DoD international cooperative projects and programs, NATO security matters, foreign disclosure matters, international transfers, and other matters based on arrangements with foreign governments and international organizations will also be coordinated with OUSD(P) Director, ISP, prior to issuance.

d. OUSD(I) CI&S informally coordinates proposed ISLs with the NISPPAC.

SECTION 4: FCLS

4.1. GENERAL. In accordance with the provisions of this section, upon receiving a valid FCL request, DSS will process an FCL at the appropriate level and determine if the company meets the eligibility requirements for access to classified information. GCAs may award a contract requiring access to classified information prior to the issuance of the FCL, but will not grant access to classified information until DSS grants the FCL. The prime contractor for a classified procurement must have a valid FCL at the highest level of classified information involved in the contract, even if a subcontractor will perform all classified activity. Contractors are authorized to possess classified material at their facility(ies) where they have an FCL and CSA-approved safeguarding capability at the appropriate level.

4.2. RECIPROCITY. An FCL issued by any CSA will be considered valid and acceptable for use on a fully reciprocal basis by all federal departments and agencies if it meets or exceeds the level of classified access and, as applicable, the level of safeguarding required. If a contractor in process for a DSS granted FCL or the sponsoring GCA indicates that the contractor has, or is in process for an FCL with another NISP CSA (e.g., DOE), DSS will contact the other NISP CSA, in accordance with the provisions of Paragraph 4.5.a of this volume to determine which CSA will exercise oversight.

4.3 FCL REQUEST

a. A GCA (or in accordance with DoD 5220.22-M, a contractor) must submit a request to DSS to process a prospective contractor for an FCL based on a requirement to access classified information in connection with a legitimate USG requirement. A foreign government or NATO entity may also initiate an FCL for a U.S. contractor in accordance with applicable security agreements. When actual knowledge of classified information is not required, but reasonable physical security measures cannot be employed to prevent aural or visual access, it may be necessary for a GCA to sponsor a company for an FCL, even when actual knowledge of classified information is not required, because reasonable physical security measures cannot be employed to prevent aural or visual access. The GCA will indicate such requirement in the DD Form 254. DSS provides instructions on FCL processing, as well as how to obtain on line verification and continuing updates of FCL and safeguarding capability of specific facilities at www.dss.mil. Paragraph 4.8 of this volume provides information on the types of contractor business structures and KMP considerations for FCL and personnel security clearance (PCL), respectively.

a. (Added)(AF) DCSA maintains NISS as the system of record for FCLs issued by the Department of Defense. Information regarding accessing this system is available at www.dcsa.mil. NISS may be used by contracting officers, program managers, Information Protection Offices and others to determine the level of a company's FCL, the existing classified safeguarding capability of a company, and to obtain information regarding any restrictions that may be present for the FCL.

b. DSS will not accept a request for FCL without sufficient justification and will not accept a request for FCL from the company to be cleared. An FCL request submitted to DSS should contain:

b. (Added)(AF) Requests for an FCL must be submitted electronically through NISS. (T-0) Special care should be taken to ensure all elements required by Paragraphs 4.3.b.(4)(a) through 4.3.b.(4)(g) are included in the request.

(1) The name, address, telephone number, and e-mail address of the requester, including a point of contact.

(2) The name, address (physical and mailing), and telephone number of the company to be cleared, including the name and contact information (telephone number and e-mail address) of a company official who will serve as the point of contact during FCL processing.

(3) The level of FCL (TOP SECRET (TS), SECRET, or CONFIDENTIAL) required.

(4) Justification for the request, including information regarding the nature of the tasks or services to be performed by the company that require access to classified information (see Paragraph 4.3.a of this volume). Examples of documentation that may be used to justify an FCL request include:

(a) A DD Form 254.

(b) A security aspects letter.

(c) A contract or a statement of work (SOW).

(d) A request for proposal.

(e) A request for quotation, request for information, or a broad agency announcement.

(f) A cooperative research and development agreement (CRADA).

(g) A GCA-sponsored independent research and development (IR&D) effort as described in Section 13 of this volume.

(5) Safeguarding requirements, if any.

(6) Any information of which the GCA is aware that may have an impact on the company's eligibility for an FCL (e.g., placement of the company or any of its KMP as excluded on the System for Award Management (SAM), formerly referred to as the Excluded Parties Lists System (EPLS)) at www.sam.gov, or a statement that the GCA is not aware of any such information.

4.4. U.S. COMPANY FCL ELIGIBILITY REQUIREMENTS. DSS will ensure that a company meets these criteria prior to granting an FCL:

a. The company requires access to classified information in accordance with the provisions of Paragraph 4.3 of this volume.

b. The company:

(1) Is organized and existing under the laws of any of the 50 States, the District of Columbia, or organized U.S. territories (Guam, Commonwealth of the Northern Marianas Islands, Commonwealth of Puerto Rico, and the U.S. Virgin Islands);

(2) Is located in the United States, its territorial areas, the District of Columbia or, when sponsored for an FCL, on a USG-controlled installation in accordance with Paragraph 3.8.b of this volume.

c. The company, if organized and existing as a business entity under the laws of an Indian tribe or an Alaska native entity, will also meet the following conditions:

(1) The Indian tribe or Alaska native entity under whose laws the company is chartered must have been formally acknowledged by the Assistant Secretary – Indian Affairs of the U.S. Department of the Interior, as a recognized Indian entity. DSS may also process a company owned in whole or in part by an Indian tribe for an FCL when the business entity is organized and existing under the laws of a U.S. State, the District of Columbia, or an organized U.S. territory.

(2) The business entity must have been organized, and continue to exist during the period of the FCL, under a tribal statute or code, or pursuant to a resolution of an authorized tribal legislative body.

(3) The Director, DSS, or designee, must have received and reviewed those records necessary for the Director to determine that the company is a tribally chartered business entity.

d. DSS may also process a company for an FCL that is a federally chartered tribal corporation formed when the Secretary of the Interior issues a corporate charter based on a petition from a tribe pursuant to Section 477 of title 25, U.S.C. (also known as the "Indian Reorganization Act, as amended").

e. A company that falls under the provisions of Paragraphs 4.4.b, 4.4.c, or 4.4.d of this volume will also meet the following criteria for an FCL:

(1) The parent companies at all levels of the business organization structure are either cleared or excluded from access to classified information consistent with the provisions of Paragraph 4.8 and Paragraph 4.10 of this volume.

(2) Is otherwise eligible for an FCL.

(3) Has demonstrated a commitment to integrity and lawful conduct in its business dealings.

(4) The company and its key managers have not been barred from participating in USG contracts.

(5) The company is not under FOCI to such a degree that the granting of the FCL would be inconsistent with the national interest. See Volume 3 of DoDM 5220.22 for FOCI procedures.

4.5. FCL PROCESSING REQUIREMENTS.

a. DSS will ensure FCL reciprocity in accordance with DoD 5220.22-M, if the company already has, or is in process for, an FCL (i.e., DSS will not process a company for an FCL, if another CSA has issued or placed the company in process for an FCL).

b. If FCL processing cannot be accomplished within the time limits to qualify the company for participation in the procurement action which gave rise to the FCL request, the GCA may request that DSS continue the clearance action in order to qualify the company for future classified contract negotiations of a similar nature. To continue the FCL processing, DSS must determine, in coordination with the GCA that:

(1) A lack of cooperation on the part of the company did not cause the delay in processing the FCL.

(2) There is likelihood that the company will participate in classified contract negotiations within the next 12 months and the contractor agrees to such participation.

c. When processing a company for an FCL, DSS will:

c. (Added)(AF) When the company is being processed for an on-installation FCL under the security oversight of the Installation Commander, the Information Protection Office will assist DCSA, upon request, in obtaining required documentation or information from the contractor. (T-1)

(1) Confirm that the FCL request is based on a requirement in accordance with Paragraphs 4.3.a and 4.4.a of this volume.

(2) Not process a branch or division of a company for an FCL unless safeguarding of classified information is required at the branch or division location.

(3) Obtain or confirm the information necessary to determine clearance eligibility. The process will also serve as an opportunity to educate the company on aspects of the NISP and company responsibilities pertaining to the protection of classified information.

(4) Obtain an SF 328, "Certificate Pertaining to Foreign Interests," located at http://www.esd.whs.mil/Portals/54/Documents/DD/forms/sf/sf0328.pdf, which has been executed by the company consistent with the provisions of DoDM 5220.22-M and mitigate or negate any FOCI in accordance with Volume 3 of DoDM 5220.22. If the company is part of a business organization, the SF 328 may be executed in accordance with the provisions of DoDM 5220.22-M with the FOCI mitigated or negated consistent with the provisions of Volume 3 of DoDM 5220.22.

(5) Obtain an executed DD Form 441 or DD Form 441-1, "Appendage to DoD Security Agreement" as applicable, from the company and execute on behalf of the USG when all FCL requirements are satisfactorily completed.

(6) Review the exclusions on the SAM to determine if the company or any of its KMPs are on the list.

(a) If the company or its KMP are not on the list, there is no impact on the FCL processing.

(b) If the company or its KMP are on the exclusions list on the SAM and depending upon the terms of the placement, DSS will:

1. Contact the Component or GCA who placed the company or its KMP to discuss the conditions of the placement on the exclusions list on the SAM.

2. Determine, in consultation with the GCA FCL sponsor and the Component or GCA who placed the company or its KMP on the exclusions list on the SAM if the FCL processing should be discontinued.

3. Notify the GCA FCL sponsor, in coordination with the Component or GCA sponsor for the contractor exclusion on the SAM whether DSS will continue the FCL processing with or without conditions; or will discontinue FCL processing.

(7) Verify PCL processing is initiated for KMP, as appropriate.

(8) Conduct and document reviews of public and government information sources to validate clearance-relevant information the company has provided, and to note and consider other information relevant to the company's qualifications for the FCL in accordance with the provisions of this section.

(9) Verify appropriate security procedures are established and implemented.

(10) Approve appropriate storage capability, if required.

(11) Advise the requesting GCA or prime contractor in writing when the FCL or

interim FCL has been granted.

4.6. INTERIM FCLS

a. DSS will consider all FCL requests for eligibility for an interim FCL and grant as soon as all requirements are met. DSS will issue an interim FCL when the KMPs have been determined to be eligible for interim PCLs at the appropriate level, FOCI has been favorably adjudicated, and all other requirements for an FCL have been met.

b. An interim SECRET or interim CONFIDENTIAL FCL is valid for access to classified information at the level of the interim FCL granted, except for access to communications security (COMSEC), Restricted Data (RD), or NATO information. See Paragraph 5.6.e.(3) of this volume about eligibility for SAP information or SCI.

c. An interim TS FCL is valid for access to TS information; except that it is only valid for access at the SECRET and CONFIDENTIAL levels for access to COMSEC, RD or NATO information. See Paragraph 5.6.e.(3) of this volume about eligibility for SAP information or SCI.

d. When DSS determines that an interim FCL has been issued in error or KMP are no longer eligible for an interim PCL, DSS will withdraw the interim FCL and final clearance processing will continue. If contract performance began under an interim FCL, prior to withdrawal of interim FCL, DSS will coordinate with the applicable GCA for guidance regarding the disposition of classified material and equipment in the possession of the contractor that must be retrieved, sanitized, or destroyed.

4.7. ISSUANCE OF THE FCL.

a. DSS will issue the FCL when KMPs are eligible for PCLs at the appropriate level, any elements of FOCI have been favorably adjudicated, and all other FCL requirements in this volume have been met.

b. DSS will notify the requester electronically when an interim or final FCL clearance has been granted.

4.8. BUSINESS STRUCTURES AND KMP CONSIDERATIONS FOR AN FCL.

a. DSS will review a company's business structure and obtain applicable governing, ownership and management documentation based on that review when processing an FCL. Business structures require different levels of analysis to determine their impact on the FCL process.

(1) Depending on the business structure and the terms of the applicable business governance documents, DSS will require the contractor to formally exclude all parent

companies or other business organizations from access to classified information or access to classified information at a lower level than the FCL of the subsidiary, as needed, in accordance with Paragraph 4.10 of this volume.

(2) There are also varying requirements, depending upon the business structure as described in this section, to determine whether the KMP will be cleared, or excluded from access to classified information in connection with the FCL. Only U.S. citizens are eligible for clearance eligibility determinations. See Volume 3 of DoDM 5220.22 for the criteria and definition for a limited FCL.

(3) If the company business structure is not addressed in this section, DSS will consult with OUSD(I) CI&S about the FCL and KMP personnel clearance considerations prior to processing the FCL.

b. With respect to KMP, regardless of the business structure, DSS will, as a minimum:

(1) Clear the facility's senior management official (SMO), for a personnel security clearance i.e., the official whose status as the SMO for a branch or division is designated by the facility or who is determined to be the SMO by DSS review and analysis of the facility's business structure and applicable governance, ownership and management documentation considering the following criteria:

(a) The SMO must have the ultimate responsibility and authority to direct actions necessary for the facility's safeguarding of classified information (even if the access to classified information by the facility's employees is solely at other contractor facilities or government locations). The SMO is normally appointed by, and reports directly to, the Board of Directors or equivalent oversight or governing body at business with such a governing or oversight body.

(b) The SMO must remain fully informed regarding the facility's classified operations and empowered to make authoritative and binding decisions based on classified threat reporting with thorough knowledge, understanding and appreciation of the information and the potential serious impacts caused by a loss of classified information. The SMO has a degree of accountability for the management and operations of the facility that cannot be obtained by any delegation of SMO responsibilities to a subordinate official at a facility.

(2) Clear the facility security officer (FSO) and the contractor's insider threat program senior official in connection with the FCL.

(3) Process for security clearances any individuals, including shareholders, members or partners, to the level of the FCL as a KMP, if DSS determines that said individuals are exercising management authorities over the facility.

(4) All other KMP (e.g., other officers, directors, partners, joint venturers, or similar company officials) who do not require access to classified information and do not occupy positions that would enable them to adversely affect the organization's policies or practices in

the performance of classified contracts will be formally excluded from clearance requirements in accordance with Paragraph 4.10 of this volume. Depending upon the circumstances of the business organization and the requirement for access to classified information, DSS may determine that some KMP can be processed for PCLs at a lower level than the FCL provided those KMP do not occupy positions that would enable them to adversely affect the organization's policies or practices in the performance of classified contracts.

c. DSS will take FCL and KMP clearance-related actions in accordance with the provisions of this volume depending upon the business structure of the company as follows (see Paragraphs 4.5, 4.6, 4.7, and Paragraph 4.8.b of this volume for additional guidance):

(1) Multiple Facility Organization (MFO)

(a) Process the home office (HOF) of an MFO for an FCL at the same or higher level than the branch or division. Clear the senior management official.

(b) Require the HOF to execute the DD Form 441 and SF 328.

(c) Require the HOF to execute a DD Form 441-1 for the cleared branch or division.

(d) Do not process an MFO branch or division office for an FCL if it does not have a need to store classified information.

(2) Corporation

(a) Determine if the corporation has a parent entity.

(b) Unless the parent has a legitimate USG or foreign government requirement requiring access to classified information, require the corporation to formally exclude the parent from access to classified information.

(c) If the parent has a requirement to perform on a classified contract, only at a lower level than the corporation, require the corporation to formally exclude the parent entity from access to classified information at the higher level.

(d) Clear the chair of the board in connection with and at the level of the FCL.

(e) Clear all directors who could fill the chair at the level of the FCL if there are provisions in the by-laws for rotating the position of chair among the directors. Issuance of the FCL will depend only on issuance of a PCL for the current chair.

(3) Limited Liability Company (LLC)

(a) Obtain copies of the LLC's "Certificate of Formation" or "Articles of Organization" on file with the State government and determine:

1. Identification of the LLC members.

2. Duration of the LLC as well as the extent to which members can transfer, sell, pledge, or take other related actions with their ownership interests, and the rights that transferees obtain.

(b) Determine if the LLC is qualified to do business in other States.

(c) Obtain copies of any written agreements between LLC members that describe the entity and the members' understanding about its operation.

(d) Clear the chair of the board of managers or chair of the board of members if the LLC is member-managed.

(e) Clear the members (whether company or individual) that are empowered to enter into contracts on behalf of the LLC, in connection with the FCL.

(4) Partnership

(a) Evaluate the provisions of the partnership agreement. As a general rule, all general partners must be cleared for PCLs or FCLs at the same level as the FCL of the partnership.

(b) As an exception to all general partners being cleared, clear the members of a legally constituted executive committee at the same level as the FCL, if the partnership has fully delegated management duties and responsibilities to the committee, and clear the chair of this committee for a PCL at the same level and in connection with the FCL.

(5) Sole Proprietorship. Clear the owner and the FSO in connection with the FCL.

(6) Joint Venture (JV)

(a) Determine under what form of business organization the JV will operate (e.g., LLC, corporation, or partnership). This will require an analysis of the JV agreement, which should also indicate the authority of any of the joint venturers to direct or decide matters affecting the JV business organization. Depending on the JV business structure, the terms of the JV agreement, and the clearance status of the joint venturers, DSS will require exclusion action(s) as needed.

(b) Determine whether the JV has a contract requiring access to classified information. Determine if any of the joint venturers have contracts requiring access to classified information in accordance with Paragraph 4.3 of this volume, and if necessary, in coordination with the applicable GCA or prime contractor.

(c) Process the JV for an FCL in accordance with the provisions of this section if it requires access to classified information. Process the joint venturer(s) requiring access to

classified information for an FCL, in accordance with the provisions of this section.

(d) In some cases, the JV may not have any employees other than the FSO, if the joint venturers teamed to perform on a specific program, project, or contract. The JV agreement will detail the terms under which the joint venturers have agreed to provide their employees to perform the required tasks, and the terms of the contract will determine whether such tasks require FCLs and PCLs. For purposes of exchange of classified information and visits among the joint venturers, the general rules applicable to the exchange of classified information and visits between prime and subcontractors will apply.

(e) Any joint venturer that does not require access to classified information will be formally excluded by those joint venturers who do require access to classified information.

(7) Colleges and Universities

(a) Clear the chair of the board and all board members (sometimes referred to as regents) who are eligible for or could sit as pro tem (temporary) board chair at the same level as the FCL.

(b) Clear all members who could fill the chair, if there are provisions for rotating the position of chair among the board members. Issuance of the FCL will depend on issuance of the PCL at the same level as the FCL for the current chair of the board.

(c) Clear the chair of a legally constituted executive committee, if the board has delegated certain of its duties and responsibilities to said committee.

(8) Self-incorporated Consultants. A self-incorporated consultant is only eligible for an FCL if the consultant and at least one other employee of the consultant's company require access to classified information. Such cases would constitute a legitimate requirement for an FCL in accordance with Paragraph 4.3 of this volume, and as such, a DD Form 254 must be issued by the GCA or prime contractor, and DSS will process the consultant's company for an FCL. See Paragraph 5.8 of this volume for guidance on when a self-employed consultant to a contractor is cleared only as an individual.

(9) Temporary Help Supplier

(a) Conduct a detailed analysis of the business structure of the temporary help supplier, the employer-employee relationships, and the classified contract information to determine the entity to be granted the FCL. Process the FCL in accordance with the business structure of the temporary help supplier and the provisions of this section.

(b) In some cases, the temporary help supplier awarded the classified contract is a licensee or franchise holder. The DSS determination of the type of licensee or franchise holder (referred to in this volume as "licensee") will guide how DSS will processes the FCL. The three types of licenses are:

1. A temporary help supplier grantor (referred to in this volume as "grantor") awards a license or franchise to a licensee, which is a legal entity separate and distinct from the grantor to do business under the name, method of operation, or style of the grantor (e.g., doing business as). The temporary help personnel are actually employees of and on the payroll of the licensee. DSS will process this type of temporary help supplier for an FCL in the same manner as any other U.S. company in accordance with the provisions of this section.

2. The grantor issues a license or franchise to other individuals or firms to use the grantor's personnel for administrative support. In this case, since the temporary help supplier personnel are employees of, and on the payroll of the grantor, normally there would be no valid basis for DSS to process the licensee for an FCL. But, as an alternative, DSS may process an FCL in the name of the grantor at the licensee's address if there is a valid requirement for employees of the grantor to have access to classified information provided:

a. The grantor has an FCL at its HOF.

b. An employee of the grantor, located on the premises of the licensee is the FSO for the grantor; or,

c. The grantor and at least one or more employees of the licensee establish an employer-employee relationship through the execution of a separate written agreement between the parties or by insertion of a clause in the franchise or license agreement. That clause must specify that one or more employees of the licensee will act as the FSO for the grantor in the territory covered by the license or franchise.

3. A grantor issues license or franchise to other individuals or firms to use the method of operation or style of the grantor in a specific geographic area. The temporary help personnel are actually employees of and on the payroll of the licensee. DSS will process this type of temporary help supplier for an FCL in the same manner as any other U.S. company in accordance with the provisions of this section.

(c) If a licensee has license or franchise agreements with more than one grantor, DSS may process an FCL in the name of each grantor provided there is a valid requirement for access to classified information. Similarly, if a contractor is engaged in a business that requires an FCL in connection with that business and is also a licensee for a temporary help supplier, DSS may process an FCL for the contractor's business and another FCL in the name of the grantor.

(10) Commercial Carriers

(a) Verify that the Surface Deployment and Distribution Command (SDDC) submitted the FCL sponsorship request for a SECRET FCL for eligibility to ship SECRET and CONFIDENTIAL material.

(b) Verify that the contractor provided SDDC with a tender, agreement, or contract under which the contractor will provide protective security service.

(c) Process the FCL based on the commercial carrier's business structure in accordance with this section.

(d) Verify to SDDC if the FCL is granted or if the company is not eligible for an FCL.

(11) Commercial Destruction Facilities. Commercial destruction facilities (mobile or stationary) are not required to be cleared when contractor personnel are authorized to perform all portions of the destruction and visual access can be controlled. If destruction facility personnel must perform the destruction, the facility is required to be processed for an FCL. See procedures for use of destruction facilities in Paragraph 7.5 of this volume.

(12) Franchises. See FCL procedures in Paragraph 4.8.c.(9) of this volume.

(13) Freight Forwarders (FF)

(a) Verify that a GCA, a U.S. contractor, or a foreign government sponsored the FF FCL.

(b) Verify that a cleared FF is registered with the Department of State (DoS), since FF activities are considered "exports" pursuant to the ITAR, because they handle international transfers of U.S. or foreign government classified material to U.S. or foreign recipients.

(c) Do not process an FF for an FCL if the FF only processes unclassified paperwork and makes arrangements for the shipment of classified material to foreign recipients and never has possession of a classified consignment.

(d) Process an FF for use by multiple countries only if:

1. The National Security Authority or designated security authority (DSA) (referred to collectively in this volume as DSA) of the government of each country using the FF, Defense Security Cooperation Agency (DSCA), and OUSD(P) Director, ISP, provide written approval for such multiple country use each time a different country proposes to use the same FF.

2. The DSS written request for approval to each DSA, DSCA, and OUSD(P) Director, ISP, includes information on the ownership of the FF (to include FOCI and any FOCI mitigation), as well as each country wanting to use the FF.

(e) Process the FCL based on the FF's business structure in accordance with this section and the determination of which of the three FF types are involved:

1. An FF that is a U.S.-owned business, organized and existing under the laws of any of the 50 States, the District of Columbia, or organized U.S. territories to do business in the United States. DSS will process this type of FF for an FCL in the same manner as any other

U.S. company in accordance with the provisions of this section.

2. An FF that is organized and existing under the laws of any of the 50 States, the District of Columbia, or organized U.S. territories, and located in the United States, the District of Columbia, or U.S. territorial areas (i.e., is legally a U.S. company), but considered to be under FOCI based on the elements of FOCI analyzed by DSS. DSS will process this type of FF for an FCL in accordance with the provisions of this section and provided the FOCI can be mitigated or negated in accordance with the provisions of Volume 3 of this manual. When the FF is not cleared through the auspices of a Voting Trust or Proxy Agreement, DSS will inform any third- party government wanting to use the FF to handle classified consignments of the FOCI mitigation circumstances in writing. The third-party government must, in turn, consent in writing prior to the use of the FF. If this FF will only handle classified consignments for the government of the foreign owner, DSS may clear it through the auspices of a limited FCL in accordance with the provisions of Volume 3 of this manual, in response to a request by the foreign government.

3. An FF that is registered to do business in the United States, but is legally organized in another country. This type of FF is a foreign company. Such business entities normally would not be eligible for an FCL. However, if the government of this foreign company requests that the element of the company operating in the United States be cleared under the NISP to handle classified shipments for that government and provides a facility security assurance for the foreign company, DSS may process the company's location in the United States for a limited FCL in accordance with the provisions of Volume 3 of this manual and only verify the limited FCL to the sponsoring foreign government. The foreign owners may assign employees from the foreign parent company to work at the U.S. location. If those employees require access to classified material, DSS will obtain a security assurance on each such employee from the government of the foreign parent company in accordance with provisions of the applicable bilateral or multi-national international agreements.

(f) Clear the U.S. citizen FSO, the U.S. citizen insider threat senior official, and U.S. citizen senior management official of the first two types of FFs (in accordance with this section) at the level of the FCL.

(g) Obtain a PCLSA for the senior management official KMP, if the FF is a foreign company (in accordance with the third type of FF in this section) and the foreign owner assigns a cleared citizen of that country to serve as a KMP requiring a PCL. The security assurance for the KMP from the foreign government will be requested in accordance with provisions of the applicable bilateral or multi-national international agreements. The FSO and insider threat senior official will always be cleared U.S. citizens.

(h) Take the following actions when a company is no longer designated to serve as an FF and there is no other reason to maintain the FCL:

1. Notify the SDDC and Defense Logistics Agency, Defense Logistics Management Standards Office of the change in designation.

2. Invalidate the FCL.

3. Initiate action to administratively terminate the FF's FCL with 30 days prior written notice.

(14) Law Firms. When legal services require access to classified information, gather information regarding FCL or PCL sponsorship, the nature and extent of the legal services to be provided, and then determine whether to process the law firm for an FCL or an individual attorney for a PCL.

(a) Legal Counsel for Criminal Proceedings. Consistent with provisions of DoDM 5200.02, in criminal proceedings where non-federal legal counsel may require access to classified information, Section 1, et.seq., of Title 18, U.S.C., Appendix 3 (also known as the "Classified Information Procedures Act, as amended")) applies. DSS may, as necessary, coordinate any requests for either FCLs or PCLs in such instances with the court, Department of Justice, Judge Advocate General of the affected military component, or with the Office of the General Counsel of the Department of Defense before taking action.

(b) Legal Counsel for Civil Litigation. The applicable Component or affected GCA will determine whether there is a legitimate need-to-know requirement for access to classified information by counsel representing parties involved in actions in which the U.S. Government is a party. In those instances where the legal counsel is an outside law firm or individual attorneys instead of in-house attorneys of a cleared company, an authorized official of the GCA will determine if the outside legal counsel requires access to classified information. In instances when the GCA has determined that access to classified information by outside counsel is required for a specific matter, DSS will process the law firm for an FCL and the law firm may submit requests for PCLs for any of the law firm's attorneys or support personnel who require access to classified information. In instances where a law firm cannot or will not be granted an FCL, individual attorneys employed by the law firm who require access to classified information may be processed for a PCL as consultants to the sponsoring GCA.

(c) Non-Criminal Legal Services. If legal counsel or legal services are not provided by in-house counsel for such non-criminal legal services as review of contracts, patents, etc., the law firm retained to provide such services will be processed by DSS for an FCL as a subcontractor, provided that the sponsoring contractor or GCA determines that access to classified information is required. See Paragraph 7.4.a of this volume and Paragraph 12.19.b.(2) of this volume for additional guidance on patent attorneys or patent firms.

(15) Off-Site Location. Determine whether various contractor activities dispersed among multiple locations within a defined geographical area qualify for a single FCL based on:

(a) Centralized management of the multiple locations in question and maintenance of a centrally directed security program.

(b) Whether physical separation of activities allows for effective supervision of security operations.

4.9 FOREIGN PERSONS SERVING AS OFFICERS, PARTNERS, OR MEMBERS OF BOARDS OF DIRECTORS. Companies that have foreign persons serving as partners, officers, or members of the Board of Directors may be issued an FCL if they are otherwise eligible and are found not to be under FOCI to such a degree that the granting of the FCL would be inconsistent with the national interest. DSS will require the contractor, by an exclusion action of the company's board of directors or similar executive body, to effectively and formally deny access to all classified information by the partner, officer, or director who is a foreign person and that said individual is not in a position to adversely affect the contractor's policies or practices in the performance of classified contracts. The senior management official will be a U.S. citizen.

4.10. EXCLUSION PROCEDURES.

a. DSS will ensure that KMP who do not require a PCL, or who require a PCL for access to classified information at a lower level than their companies FCL, are officially excluded from unauthorized access by means of a formal exclusion action by the company's board of directors or similar executive body. DSS will maintain a copy of the exclusion action. The following language will be used for the exclusion action, as appropriate:

(1) Such officers, directors, partners, joint venturers, regents, trustees, or similar company officials (identified by name) will not require, will not have, and can be effectively and formally excluded from access to all classified information disclosed to the organization.

(2) Such officers, partners, joint venturers, regents, trustees, or similar company officials (identified by name) will not require, will not have, and can be effectively and formally excluded from access to (specify classification level(s)) of classified information.

b. DSS will ensure that parent companies at all levels of the business organization that do not require an FCL or that require an FCL for access to classified information at a lower level than their subsidiary are officially excluded from unauthorized access by means of a formal exclusion action by the parent boards of director or similar executive bodies. As part of the exclusion process, the parent companies will complete an SF 328 consistent with the provisions of DoD 5220.22-M.

(1) If DSS determines that the immediate parent of the subsidiary should be excluded, all other parent companies in the multi-level business organization will also be processed for formal exclusion, unless an independent clearance need exists.

(2) DSS will maintain a copy of the parent(s) formal exclusion actions and the subsidiary's formal acknowledgment of those exclusions actions. The following language will be used for the exclusion action, as appropriate: each parent company will exclude itself from access to all classified information and delegate full authority to the subsidiary to act independently of the parent(s) in all matters which involve or relate to the subsidiary's responsibilities to safeguard classified information.

4.11. PCLS CONCURRENT WITH THE FCL OTHER THAN KMP. DSS may process PCLs concurrent with the FCL processing for contractor employees who require access to classified information during the pre-award phase of a procurement action or at the start of a contract. The DoD CAF may issue PCL eligibility prior to issuance of the FCL. GCAs will not grant access to classified information to the contractor and its personnel until the FCL has been granted in accordance with the provisions of this section. The granting of an FCL by DSS is not dependent on the clearance of such employees. DSS will obtain information pertaining to those individuals who should be processed for PCLs concurrent with FCL processing during their initial visit to the contractor.

4.12. ADMINISTRATIVE TERMINATION AND DOWNGRADING OF AN FCL.

a. When a contractor has not participated in a classified procurement effort for a 12-month period, has not been afforded authorized access during the preceding 12 months, and has no immediate prospects for obtaining a classified contract, DSS will administratively terminate the FCL after giving the contractor 30 days written notice.

a. (Added)(AF) For on-installation cleared facilities, the Installation Commander will request DCSA to administratively terminate the FCL for the on-installation location when there is no longer a requirement for classified work to be performed at that location. (T-0) Commanders will submit requests through MAJCOM information protection channels. (T-1)

b. When a contractor has not had a classified contract or project for the preceding 12 months, but has classified material in its custody, DSS will request that the GCA who approved the retention verify the continuing requirement for the contractor to retain custody of the classified material. If the GCA does not verify a continuing requirement for the FCL, DSS will arrange for the appropriate disposition of the classified material in question and proceed with administrative termination of the FCL. DSS will request the assistance of the GCA and if applicable, the National Security Agency/Central Security Service (NSA/CSS) in accordance with Paragraph 13.5 of this volume, if the contractor refuses to dispose of classified material in its possession. The GCA will take action to retrieve its classified material from the contractor and assist DSS in verifying that the contractor has appropriately disposed of all classified material. DSS will then proceed with administrative termination of the FCL.

b. (Added)(AF) For on-installation cleared facilities proposed for administrative termination of the FCL, the Information Protection Office will conduct a close-out inspection prior to the administrative termination of the FCL by DCSA. (T-1) The Information Protection Office will also conduct a close-out inspection for independent visitor groups safeguarding classified material. (T-1) The close-out inspection must include a thorough check of all areas and containers authorized for storage of classified material to ensure all classified items in the possession of the contractor are properly secured and returned to the government prior to FCL termination. The program office, requiring Air Force activity, or contracting officer will notify the Information Protection

Office in writing a minimum of 30 calendar days prior to expected completion or termination of contract performance. (T-1)

c. DSS will evaluate the need for continuation of an FCL at the TS level and administratively downgrade the FCL, if there has been no possession of or access to TS information, and no bid, quote, or proposal submitted by the contractor in response to a legitimate requirement during the preceding 1-year period that would have required contract performance at the TS level.

d. If the GCA provides justification for continuation of an otherwise inactive FCL, the GCA will revalidate that justification annually in writing to DSS if the GCA has a requirement to continue the FCL.

4.13. CHANGED CONDITIONS AFFECTING THE FCL. DSS and the applicable GCA will take the appropriate actions in accordance with this section when notified of any change concerning the contractor that could affect the FCL provided the contractor has a current procurement requirement for access to classified information or possesses classified information.

4.13. (Added)(AF) The GCA will notify DCSA through the servicing Information Protection Office when made aware of any change concerning a contractor that could affect the FCL. (T-1) Examples of reportable information are provided in Paragraphs 4.13.a. through 4.13.l.

a. Change of Operating Name. If ownership and management remain the same, DSS will:

(1) Execute a new DD Form 441 or DD Form 441-1, as applicable.

(2) Update the FCL information in the ISFD, or successor system.

b. Change in Management. DSS will:

(1) Initiate PCL action for the new KMP, if appropriate.

(2) Coordinate with the GCA regarding the continued retention of classified material unless assured that it can be appropriately safeguarded and that the new management is effectively and formally excluded from access to the classified information while PCLs are being processed.

c. Change in Ownership. DSS will:

(1) When classified material or contracts are involved in the proposed sale of all or part of the assets of a contractor, process the buyer for an FCL. If the proposed sale would place the contractor under FOCI, follow the procedures provided in Volume 3 of this manual.

(2) If classified information cannot be protected from unauthorized access prior to consummation of the sale and transfer, invalidate the FCL and coordinate with the GCA to recover all classified information from the contractor.

(3) When a merger or consolidation occurs and one of the corporations involved is either cleared or excluded, in accordance with the provisions of this section, formally exclude the surviving corporation or process the surviving corporation for an FCL.

d. Change of Address. When a contractor relocates or when the change involves only a change of address, with no relocation of any elements of the contractor (e.g., such as post office change, change of zip code), DSS will:

(1) Amend the existing DD Form 441 or DD Form 441-1 as appropriate to reflect the change in address of the contractor or execute a new DD Form 441 or DD Form 441-1.

(2) Update the FCL information in the Industrial Security Facility Database, or successor system.

(3) When a possessing contractor relocates, DSS will conduct an on-site visit to assess the contractor's security procedures and safeguarding capabilities, at the new location. DSS may also conduct an onsite visit during the relocation process.

e. Business Closing. Ensure that all classified material has been appropriately returned or destroyed. DSS will administratively terminate the FCL in all instances in which a company previously granted an FCL has gone out of business or has ceased to operate the business for any reason.

f. Bankruptcy

(1) DoDM 5220.22-M requires contractors to report bankruptcy. GCAs will notify DSS if the GCA learns that a contractor is undergoing imminent adjudication or reorganization in bankruptcy to allow DSS to verify that the contractor reported such a change to DSS.

(2) If a contractor is undergoing imminent adjudication of or reorganization in bankruptcy (e.g., Chapter 7, 11, or 13), DSS will ensure that all classified material is appropriately protected, returned, or destroyed in coordination with the applicable GCAs. The Components or applicable GCAs must assure disposition in accordance with the approved records disposition of the specific Component or GCA supported by the contract effort.

g. Placement of Contractor as Excluded on the SAM

(1) Components and GCAs will notify DSS when placing a contractor or any of its employees as excluded on the SAM (www.sam.gov) in order for DSS to determine impact on the applicable FCL.

(2) DSS will invalidate an FCL when notified by a Component or GCA of placement of

a contractor as excluded on the SAM or when DSS becomes aware of a contractor's placement as excluded on the SAM. If the exclusion involves KMP, DSS may invalidate the FCL, if the KMP are required to be cleared as part of the FCL. If the exclusion involves contractor employees other than KMP, DSS will determine, in consultation with the applicable Component or GCA, if the FCL should be invalidated.

(3) Generally, as long as DSS determines, in consultation with the applicable Component that the invalidation should continue, the contractor is ineligible for access to additional classified information or to be awarded new classified contracts. The affected Components or GCAs will determine whether the contractor may continue to perform on existing classified contracts or have access to additional classified information for those existing contracts consistent with subpart 9.4 of the FAR and their Component or GCA specific procedures and notify DSS.

(4) The applicable Component head may determine that there are compelling reasons to issue a new classified contract consistent with the FAR. In such instances, the Component head must provide DSS with the compelling reason consistent with the FAR and any Component or GCA specific procedures related to the compelling reason, (e.g., what additional security procedures the contractor must implement while performing on the classified contract). DSS will consult with the GCA about the adequacy of any additional security procedures, as well as, whether the FCL invalidation should remain in place, while the contractor has a new classified contract or access to additional classified information based on the Component head's compelling reasons.

h. Changes Involving a Parent Organization. When the FCL of a parent organization is terminated, DSS will invalidate and ultimately terminate the FCLs of the subsidiaries unless the parent is formally excluded.

i. Changes Involving an MFO. Before terminating the clearance of the HOF of an MFO, DSS will:

(1) Consult with the applicable GCAs regarding any continued classified contract performance requirements by cleared facilities within the MFO.

(2) If there are no requirements to retain any FCLs within the MFO, confirm the disposition of any classified holdings with the applicable GCAs. The Components or applicable GCAs must assure disposition in accordance with the approved records disposition of the specific Component or GCA supported by the contract effort in their confirmation to DSS about any disposition of classified holdings within the MFO.

j. Changes Involving an FF. See Paragraph 4.8.c(11) of this volume for actions involving changes to FFs.

k. Upgrading of an FCL. DSS will:

(1) Confirm that the contractor will submit the KMPs for PCLs and update the FCL

when all PCLs are ready to be issued.

(2) Update the FCL information in the ISFD, or successor system.

l. Other Changes That Could Impact FCL Eligibility.

(1) Components or their GCAs will notify DSS of any information that adversely reflects on the integrity or character of a contractor or the contractor's KMP, that suggests the contractor's ability to safeguard classified information may be impaired, or that the contractor's access to classified information clearly may not be in the interest of national security.

(2) DSS will:

(a) Consult with the applicable Component or GCA in its process to decide what FCL action to undertake based on the information reported and the provisions of this section.

(b) Advise the applicable Component or GCA of the DSS decision regarding the contractor's FCL eligibility.

4.14. PERSONNEL ACTIONS AFFECTING AN FCL. When the eligibility determination for an individual who is required to be cleared in connection with an FCL is denied, revoked, suspended, or withdrawn, then the FCL will be denied, invalidated, or revoked accordingly, unless the contractor has taken immediate action to remove the individual from their official position and effectively and formally excluded that person from access to all classified information.

4.14. (Added)(AF) On-installation contractor activities, cleared facilities, and visitor groups will report adverse information regarding individual contractor employees in accordance with paragraphs 2.7.h.(1) through 2.7.h.(3). (T-1)

a. DSS will consider the following when making a determination of the contractor's assurances of exclusion from access:

(1) The seriousness of allegations that led to the suspension of the eligibility.

(2) The actions that the contractor has taken to relieve the official from authority and influence over operations of the contractor.

(3) The degree to which the individual has been removed from access to classified information (e.g., removed the individual from access in the DoD personnel security system of record).

b. If the contractor does not take appropriate action to remove or exclude the individual from access:

(1) DSS will:

(a) Invalidate the FCL and ensure protection of all classified information or its disposition in accordance with the provisions of Paragraph 4.15 of this volume.

(a) (Added)(AF) When the Installation Commander provides oversight of on-installation cleared facilities, the Information Protection Office will provide oversight of the protection of all collateral classified information in the contractor's possession. (T-1)

(b) In consultation with the applicable GCA(s), revoke the FCL in accordance with the provisions of paragraph 4.17 of this volume.

(2) The GCA will, in accordance with the provisions of paragraphs 4.15 and 4.17 of this volume:

(2) (Added)(AF) The Air Force GCA (e.g., contracting officer, program manager, Program Executive Officer, etc.) will take the actions identified in Paragraphs 4.14.b.(2)(a) and 4.14.b.(2)(b) and provide a copy to SAF/AAZ through MAJCOM information protection channels. (T-1)

(a) Determine whether to terminate or continue the contract and advise the applicable DSS field office of the decision.

(b) Coordinate with the DSS field office, annotated on the DD Form 254, to ensure appropriate disposition of all classified information in the contractor's possession.

4.15. INVALIDATION OF AN FCL.

a. DSS will invalidate an FCL in accordance with the provisions of this section, if there is a changed condition or non-compliance with other requirements as set forth in DoD 5220.22-M that affect the ability of a contractor to adequately protect classified information.

b. When changed conditions occur pertaining to a contractor, the first consideration will be the safeguarding of classified information to which the contractor has current or impending access. DSS will take action to ensure the safeguarding of the classified information immediately upon an initial determination that conditions have changed. FCLs will not be invalidated immediately because of changed conditions if:

(1) DSS determines that classified information in the contractor's possession can be adequately safeguarded.

(1) (Added)(AF) When the Installation Commander provides oversight of on-installation cleared facilities, the Information Protection Office will provide a recommendation to DCSA regarding the contractor's ability to provide adequate safeguarding of classified information in their possession. (T-1)

(2) In the case of a change of management, the new KMP will be effectively and formally denied access to classified information pending completion of PCL actions and required PCL forms are promptly submitted for processing. If new KMP are not expected to be cleared within 30 days, DSS will obtain an exclusion certificate in accordance with Paragraph 4.10 of this volume as an assurance of the contractor's intent to deny access to the uncleared KMP.

(3) In the case of FOCI, the contractor notified DSS prior to the changed condition and has submitted an acceptable FOCI action plan in accordance with DoD 5220.22-M. See Volume 3 of DoDM 5220.22 for FOCI procedures.

c. If it is necessary to invalidate the FCL:

(1) DSS will:

(a) Provide the contractor with immediate written notice that includes the reasons, ramifications, and required actions to bring the FCL back into a valid status, along with a specific time frame for corrective actions.

(b) Notify all stakeholder activities that have classified contracts with the contractor and all activities that have verified the FCL and safeguarding capability within the last year of the invalidation.

(c) Inform the GCA with current classified contracts, (i.e., the program manager, or contracting officer's representative, and industrial security point of contact) of the specific reasons for the invalidation (e.g., for a changed condition or due to the non-compliance from a security review) in sufficient detail to the GCA. Notify the NSA/CSS, as applicable, consistent with the provisions of Paragraph 13.5 of this volume.

(c) (Added)(AF) SAF/AAZ serves as the Air Force industrial security point of contact and receives invalidation notifications from DCSA. Upon receipt, SAF/AAZ will provide notification through MAJCOM information protection channels to ensure the GCA (e.g., program manager, contracting officer) is aware of the FCL invalidation, understands the root cause for the action, and considers appropriate action. (T-1)

(d) Request decision from the GCA as to whether or not the contractor may continue to perform on its existing contracts pending resolution of the security issues caused by the changed condition.

(2) GCA will:

(a) Review the details of the invalidation provided by DSS and make a risk management decision whether or not the contractor should be permitted to continue performing on their classified contracts, to include the ability to issue new subcontracts.

(b) Provide DSS with the GCA's formally documented decision as described in Paragraph 4.15.c.(2)(a) of this volume within 15 days.

(b) (Added)(AF) The GCA will ensure a copy of the memorandum documenting the decision is provided to SAF/AAZ through MAJCOM information protection channels. (T-1)

(c) Coordinate with DSS regarding the recovery of classified and related unclassified material, if necessary.

4.16. REVALIDATION OF AN FCL. Once DSS determines that the situation that caused an invalidation of the FCL has been corrected, in accordance with the provisions of this manual, DSS will revalidate the FCL and notify all activities that were advised of the invalidation action that the invalidation has been lifted. If DSS determines that the situation that caused the invalidation of the FCL has not been corrected, DSS will not revalidate the FCL.

4.16. (Added)(AF) Upon receipt of revalidation notifications, SAF/AAZ will communicate the notification through MAJCOM information protection channels to ensure the GCA is aware of the revalidation of the FCL. (T-1)

4.17. REVOCATION OF AN FCL. If the contractor refuses or is unable to take action to correct the situation that caused invalidation or has consistently demonstrated an unwillingness or inability to properly protect classified information:

a. The GCA(s) will:

(1) Determine whether the national security interest is best served by permitting contract completion instead of revocation action.

(2) Determine if and how any subcontractors should continue contract performance upon revocation of a prime contractor's FCL.

(3) Coordinate with DSS to ensure the appropriate disposition of classified and unclassified related material prior to revocation action. The Components or applicable GCAs must assure disposition in accordance with the approved records disposition of the specific Component or GCA supported by the contract effort.

(4) Provide DSS with a decision, in writing, within 15 days from the DSS request to revoke the FCL.

(5) Consult or coordinate with DSS, if the GCA's formal decision is that contract performance will continue instead of revocation, to determine the procedures to be followed to protect any remaining classified information until contract completion, in accordance with Paragraph 4.17.b(2) of this volume.

(6) (Added)(AF) The GCA will coordinate with Information Protection Offices

when making these determinations and will provide a copy of the memorandum documenting the decision to SAF/AAZ through MAJCOM information protection channels. (T-1)

b. DSS will:

(1) In consultation with the appropriate GCAs, NSA/CSS, and the DoD SAPCO, as applicable, revoke the FCL, revoke all accesses associated with the revoked FCL, and coordinate with all affected GCAs to ensure that classified information in the possession of the contractor is properly safeguarded, until it is removed.

(2) Coordinate with the GCA(s) to determine the procedures to be followed to protect any remaining classified information in the possession of the contractor until contract completion, if a GCA determines that it is in the best interest of the USG to permit contract completion instead of a revocation action.

(3) Notify any other contractor affected by the GCA's decision (e.g., a contractor working as a subcontractor on the classified contract(s)).

(4) Notify Defense Contract Management Agency and Defense Contract Audit Agency of the facility clearance revocation to assure that any issues that could impact auditing or contract administration with the revocation are considered.

(5) Notify any other contractor having a classified contract with the contractor in question if the company's FCL is being revoked.

(6) Ensure appropriate disposition of all other classified material prior to the revocation action.

(7) Notify all GCAs and companies that have verified the FCL of the contractor, via the system of record, within the past year, or have requested to be notified of FCL changes, of the revocation action.

(8) Terminate the contractor's FCL in accordance with Section IV of the DD Form 441 or DD Form 441-1.

c. If the contractor subsequently takes corrective action, and the GCA submits a new FCL request, DSS may process the company for a new FCL.

4.18. MAINTENANCE OF CONTRACTOR INFORMATION.

a. DSS is the office of record for the maintenance of all information pertaining to contractor FCL records and information about all contractors under its cognizance. This information is used to respond to all inquiries regarding the clearance status and storage capability of contractors. It is also used to provide continuing assurance to GCAs regarding the contractor's ability to protect classified information. (Appendix 4A of this volume contains a

listing of contractor information to be maintained.)

b. DSS will retain information pertaining to the FCL, safeguarding capability and other industrial security actions in accordance with authorized Records Disposition Authority for Industrial Security Facility Case Files, National Archives and Records Administration (NARA) and Chapter 12 of Title 36, CFR.

c. (Added)(AF) When the Installation Commander provides oversight of on-installation cleared facilities, the Information Protection Office will maintain the oversight documentation described in Appendix 4A and provide copies to DCSA as required by this volume. (T-1)

APPENDIX 4A: DSS MAINTENANCE OF CONTRACTOR INFORMATION

4A.1. Information to be maintained by DSS in accordance with Section 4 of this volume, includes, but is not limited to:

a. Basic FCL and storage capability information:

(1) Company legal name.

(2) Company alias names and prior names.

(3) Commercial and government entity code.

(4) Physical address.

(5) Unclassified mailing address.

(6) Classified mailing address.

(7) FSO name as well as corporate security official, overseeing NISP security matters, as applicable.

(8) Phone numbers (unclassified and secure telephone equipment, if applicable).

(9) E-mail address (unclassified and classified, if applicable).

(10) FCL level.

(11) Clearance date.

(12) Approved storage capability and level.

(13) Special accesses (depending upon sensitivity may be stored elsewhere).

(14) KMP identifying information, to include the insider threat senior official.

(15) HOF and principal management facility information, if applicable, and business structure relationships for parent and subsidiary companies throughout the chain of ownership.

(16) Approved off-site locations, if applicable.

(17) Responsible field oversight element.

(18) Industrial security representative assigned.

(19) Information systems security professional assigned.

(20) CI Special Agent.

b. Documentation of approval actions, advice and assistance provided to the contractor, security violations, administrative inquiries, last dates of the FSO's security, CI and insider threat awareness briefing of employees and the insider threat program personnel training, and any other actions and their resolution and related data; some of which may be stored separately.

c. Results or reports of security reviews (in accordance with Appendix 14A of this volume).

d. Classified contract numbers with the associated DD Forms 254 as well as the names of major programs requiring access to classified information, prime contractor information, and subcontractor information.

e. Description of the contractor's export control system and identified empowered official.

f. FOCI mitigation instrument, if applicable, as well as any national interest determinations if there is a Special Security Agreement in place. See Volume 3 of this manual for details.

g. Number of all employees.

h. Number of cleared employees by clearance level, to include PCL requirements and projections.

i. Number and country for foreign national employees or long term visitors.

j. Numbers and types of storage containers and facilities.

k. Numbers and types of classified material – documents, hardware, software.

l. Numbers and types of information system (IS).

m. Enrollment in cyber threat sharing (e.g., Defense Industrial Base Cyber Security/Information Assurance Program).

n. Applicable threat assessments, which may be stored separately depending upon protection requirements.

o. Special requirements. Certain information or documents may require specialized safeguarding and access restrictions. Such requirements may exist for critical program information (CPI) designation and countermeasures, operations security (OPSEC) requirements, designation as a critical national asset or requiring critical infrastructure protection.

p. Reports submitted or information furnished by the facility or company consistent with the provisions of DoD 5220.22-M, including individual reports and collective statistics and analysis

and resolution, which may be stored separately.

q. International involvement.

(1) Foreign classified contract information.

(2) Export authorizations.

(3) FGI on hand.

(4) Technology control plans (TCPs).

(5) Program/project security instructions.

(6) Transportation plans.

(7) Foreign visitors.

(8) Security education, support, and oversight for employees at overseas locations.

4A.2. Data elements as DSS, in consultation with OUSD(I) CI&S, may determine are needed for historical and comparative snapshots may be maintained (e.g., number and level of FCL in place or requested to date and processing times compared to the same time in one or more prior years, and list of countries of foreign ownership pertaining to FOCI mitigation instruments in place).

SECTION 5: ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION

5.1. GENERAL.

a. After a USG adjudication facility grants eligibility for classified information to which contractor personnel require access, an employing contractor complies with the provisions of DoD 5220.22-M to record said access in the approved DoD personnel security system of record.

b. The DoD CAF grants eligibility for an employee of a contractor only after the contractor has certified to DSS that there is a legitimate requirement for eligibility for access to classified information in the performance of assigned duties and the appropriate personnel security investigation (PSI) is completed and favorably adjudicated by the DoD CAF. The DOHA ultimately makes eligibility determinations (favorable or not) for those contractor employees that have been issued a statement of reasons (SOR) at the collateral level. The DoD-granted eligibility must occur before the contractor can give access to the employee as stated in DoD 5220.22-M.

c. GCAs will not provide a contractor employee with access to classified information unless:

(1) The company has the appropriate FCL for the level of classified information in accordance with Section 4 of this volume.

(2) There is a USG-granted eligibility for access to classified information at the appropriate level for that individual in the approved DoD personnel security system of record.

(3) There is a legitimate requirement for access to classified information by the employee of the contractor in the performance of assigned duties.

(4) The contractor employee has executed the SF 312.

d. Contractor personnel will not be granted access to classified information at a higher level than the overall FCL of their employing contractor (i.e., CONFIDENTIAL, SECRET, or TS).

(1) DSS does not record or verify eligibility or access to SCI or SAP information; this eligibility must be verified through applicable SCI or SAP channels.

(2) When actual knowledge of classified information is not required by contractor personnel, and reasonable physical security measures cannot be employed to prevent aural or visual access to classified information by contractor personnel, the applicable GCA indicates the requirements in the DD Form 254 for a PCL consistent with the provisions of Paragraph 6.2.a.(1) of this volume.

e. DoD 5220.22-M requires the contractor to report when an employee no longer wishes to be processed for a clearance or to continue an existing clearance. Therefore, when an employee

of a contractor makes it known on the PCL application, or otherwise formally (i.e., by the FSO), that he or she will not work on a classified contract or perform in a capacity requiring access to classified information for any reason, DSS will coordinate with the contractor's FSO and the DoD CAF, as applicable, on administrative actions to remove existing access to classified information or discontinue pending clearance eligibility. Such a statement by the contractor's employee negates consideration of the employee as a bona fide candidate for clearance because the employee will not, in fact, have access to classified information. The DoD personnel security system of record will be annotated by either DSS or the DoD CAF to explain that the administrative actions occurred based on the employee's statement.

f. See Paragraphs 6.2.a.(2)(a) and 6.2.a.(2)(b) of this volume with regard to contractor personnel requiring logical access to IS or recurring physical access to government installations when access to classified information is not required.

g. DSS makes and records interim eligibility determinations for contractor employees in the DoD personnel security system of record as set forth in Section 6 of this volume. The DoD CAF and DOHA are responsible for making and recording eligibility determinations for access to classified information in the DoD personnel security system of record, maintaining such records, requesting further investigations as required, and in coordination with DSS, preparing recommendations for suspension. DOHA ultimately makes final eligibility determinations (favorable or not) in the DoD personnel security system of record for those contractor employees that have been issued an SOR at the collateral level. When applicable, the DoD CAF notifies DSS of contractor personnel who may meet the criteria for suspension with respect to PCLs for contractor personnel requiring access to classified information when the employing contractor is under DSS cognizance in accordance with DoDD 5220.6.

h. The approved DoD personnel security system of record maintains security clearance and adjudicative determinations for military personnel, civilian employees of the DoD, consultants to Components and their GCAs, and for employees and consultants of contractors under DoD oversight. DSS will provide direction to contractors accessing the DoD personnel security system to perform PCL maintenance actions for contractor personnel within their span of control.

5.2. RECIPROCITY.

a. DoD reciprocally accepts existing clearance eligibility determinations or clearances from other USG agencies in accordance with E.O. 13467, the December 12, 2005 Office of Management and Budget(OMB) Memorandum and the July 17, 2006 OMB Memorandum, and part 732 of Title 5, CFR.

b. Any previously granted PCL or eligibility for a contractor employee, based upon a current investigation of a scope that meets or exceeds that necessary for the clearance required, will provide the basis for issuance of a new clearance without further investigation or adjudication unless significant derogatory information that was not previously adjudicated becomes known to the granting agency, the previous eligibility was granted based on an exception, condition, waiver or deviation, or there has been a break in access to classified

information greater than 24 months. This provision does not prevent an agency from reconsidering its own decision to grant eligibility or access.

(1) If the DoD personnel security system of record does not reflect eligibility for access to classified information, DSS will accept a request from the contractor indicating the organization that issued the eligibility and dates of access, if the contractor is aware that the applicant had access to classified information within the past 24 months. Once DSS has verified the eligibility, the DoD CAF will record eligibility in the DoD personnel security system of record.

(2) If DSS cannot verify the prior eligibility, DSS will notify the contractor of required actions, which may include a new investigation request.

c. Personnel who currently have access to classified information are subject to continuous evaluation consistent with DoDM 5200.02, ICD 704, E.O. 13467, E.O. 12968 and E.O. 13764.

5.3. INVESTIGATIVE REQUIREMENTS. PSIs and clearance eligibility determinations for contractor personnel and consultants who require access to classified information will be conducted in accordance with the standards and guidelines established in DoDM 5200.02.

5.4. CLEARANCE APPLICATION. DSS provides guidance to the FSO of his or her responsibility to advise the contractor personnel of the clearance application procedures to include format and submission.

5.5. PRE-EMPLOYMENT CLEARANCE ACTION. DSS may begin processing a PCL application prior to actual employment provided a written commitment has been made by the contractor and the applicant has accepted the employment offer in writing. The commitment for employment must indicate that employment will commence within 30 days of the granting of the eligibility, as annotated in DoD personnel security systems of record, that permits the employee to perform the tasks or services associated with the contract or government requirement for which the individual was hired.

5.6. INTERIM PCLS.

a. A contractor employee may be granted interim eligibility for access to classified information where official functions must be performed prior to completion of the investigation and adjudication process.

b. Interim eligibility will be valid for no more than 1 year, provided the delay in making a final determination is due to an incomplete investigation (e.g., the Investigative Service Provider is unable to complete the subject interview because the subject is deployed overseas).

c. The 1 year interim eligibility granted on an incomplete investigation may be extended for

a single period of up to 6 months upon approval by the designated Component authority when the benefit of granting or continuing access clearly outweighs security concerns. A compelling need request for an extension must be submitted when continued interim access will exceed more than 1 year. When the extensions for continued interim access for more than 1 year involve a NISP contractor, DSS must confirm that the applicable GCA has a compelling need before DSS approves the extension.

d. DSS will grant interim eligibility for access to classified information to contractor personnel in accordance with DoDM 5200.02 and the January 27, 2017 USD(I) Memorandum or its successor.

d. (Added)(AF) Within DoD, Commanders are not authorized to make interim eligibility determinations for contractor personnel under the NISP. The Director, DCSA is the sole office delegated authority to make interim clearance eligibility determinations for NISP contractor personnel. At all times, Commanders retain the authority to make access determinations for contractor personnel under the NISP regarding the classified information for which they are responsible in accordance with DoDM 5200.02_AFMAN16-1405.

e. Interim PCLs are valid for access as follows:

(1) An Interim SECRET or CONFIDENTIAL PCL is valid for access to classified information at the level of the eligibility granted. It is not valid for access to COMSEC information, RD, or NATO information.

(2) An Interim TS PCL is valid for access to TS information and SECRET and CONFIDENTIAL levels for RD, NATO, and COMSEC information. An Interim TS PCL is the equivalent of a final SECRET PCL.

(3) Access to SAP information or SCI based on an interim PCL is a determination made by the granting authority. If the granting authority authorizes SCI eligibility for an employee of a contractor, the underlying collateral eligibility granted by the DoD CAF also exists unless it is suspended, denied, revoked, or until there is no longer a DoD affiliation.

f. Withdrawal of a contractor's interim eligibility will not be construed as denial, suspension, or revocation of clearance. The DoD CAF will make an adjudicative determination upon the completion of the investigation.

f. (Added)(AF) When the interim clearance eligibility of contractor personnel is withdrawn, Commander's must remove the contractor personnel from access to classified information and/or assignment to sensitive duties. (T-0)

5.7. LIMITED ACCESS AUTHORIZATION (LAA).

a. Only U.S. citizens are eligible for a clearance eligibility determination. Compelling reasons may exist for approving specific, limited access to classified information by a non-U.S.

citizen. The DoD CAF may grant an LAA for contractor employees up to the SECRET level in those rare circumstances when the non-U.S. citizen possesses unique or unusual skill or expertise that is urgently needed to support a specific USG contract, a cleared or clearable U.S. citizen is not available and investigative requirements are satisfied. PSIs for an LAA will be conducted in accordance with DoDM 5200.02. Cleared contractor requests for an LAA will be submitted through the responsible GCA to the DoD CAF, in accordance with DoD 5220.22-M.

b. An individual granted an LAA may not be granted access to:

(1) TS information.

(2) RD or Formerly Restricted Data (FRD).

(3) Information that has not been authorized for disclosure by a USG designated disclosure authority to the country of which the individual is a citizen.

(4) COMSEC information.

(5) Intelligence information. In accordance with ICD 704, a candidate for SCI access must be a U.S. citizen, and only the DNI or designee can waive this requirement.

(6) NATO information, except as follows: Foreign nationals of a NATO member nation may be authorized access to NATO information subject to the terms of the contract, if DSS obtains a NATO security clearance certificate from the individual's home country. NATO access will be limited to performance on a specific NATO contract.

(7) Information for which foreign disclosure has been prohibited in whole or in part.

(8) Information provided to the USG in confidence by a third-party government and classified information furnished by a third-party government.

c. If the GCA intends to support the request for a contractor employee's LAA, the GCA must verify the need for the LAA and endorse the letter of justification provided by the contractor to DSS. The GCA endorsement will also include a statement that the responsible designated disclosure authority has verified that the classified information at issue would be authorized for disclosure to the government of the potential employee's country of citizenship. If the GCA does not support the request, it will so state and return the denied request to the cleared contractor. For those GCA-endorsed requests, DSS, in coordination with the DoD CAF will ensure that the entire endorsement package is retained for 2 years after termination of the LAA. The GCA-endorsed contractor's letter of justification for an LAA will include:

(1) The individual's name, date and place of birth, position title, and current citizenship.

(2) A statement that a qualified U.S. citizen cannot be hired in sufficient time to meet the contractual requirements.

(3) A statement of the unusual expertise possessed by the applicant.

(4) A statement that access will be limited to a specific USG contract (specify contract number).

(5) A list of the specific material to which access is proposed (delineate as precisely as possible and identify any other GCA that may have jurisdiction over any of the material, if applicable).

(6) A statement that the classified information to be accessed is releasable to the individual's country of citizenship (disclosure determination) or that an export license has been obtained.

d. Components and GCAs should be aware that DoD 5220.22-M prohibits a contractor from assigning an employee who is a non-U.S. citizen with an LAA outside the United States on programs that will involve access to classified information. Such an assignment negates the basis on which an LAA may have been provided for the contractor's employee.

e. (Added)(AF) Refer to DoDM 5200.02_AFMAN16-1405, Section 6, for information and policy requirements when requesting LAA for contractor employees.

5.8. CONSULTANTS. There are two types of contractor consultants: those serving as consultants to Components and their GCAs and not under the purview of the NISP; or those serving as self-employed consultants to contractors in the NISP, in accordance with DoD 5220.22-M.

a. Contractor consultants to Components and their GCAs are not under the purview of the NISP and will be processed for a PCL through the applicable Component or GCA's procedures.

a. (Added)(AF) Refer to DoDM 5200.02_AFMAN16-1405, paragraph 4.4, for instructions regarding personnel security clearance procedures for contractor personnel serving as direct consultants to the Air Force.

b. In accordance with DoD 5220.22-M, self-employed consultants to contractors, who require access to classified information, must have a valid eligibility prior to the contractor granting access. In addition, DoD 5220.22-M precludes the contractor from assigning a self-employed consultant outside the United States with responsibilities requiring access to classified information.

c. For these self-employed consultants, DSS will:

c. (Added)(AF) When the Installation Commander provides oversight of on-installation cleared facilities, the Information Protection Office will perform the actions in Paragraphs 5.8.c.(1) through 5.8.c.(3). (T-1)

(1) Consider, for security oversight and the contractor's security administration

purposes, that the contractor consultant is an employee of the hiring contractor.

(2) Confirm that the consultant and the using contractor jointly execute an agreement specifying security responsibilities.

(3) Verify that the consultant does not access classified information except at the hiring contractor location, on the premises of the Component or GCA on behalf of the hiring contractor, or while on authorized visits in support of and with the approval of the hiring contractor, in accordance with the provisions of DoD 5220.22-M. (See Paragraph 4.8.c.(8) of this volume for criteria for a self-incorporated consultant to be eligible for an FCL.)

5.9. PCLSA. A written assurance from a non-U.S. citizen's government of the person's eligibility for a specified level of PCL, under that government's investigative requirements, is acceptable to satisfy U.S. investigative requirements when the U.S. scope cannot be met for an LAA. Further, a PCLSA may be necessary for a U.S.-granted PCL when a U.S. citizen has lived in another country. Several bilateral security agreements and DoDD 5230.11 recognize this need and sanction the providing of PCLSAs. DSS will request the PCLSA from other governments, when required. DSS also will provide PCLSAs on U.S. citizens to other governments, upon receipt of a valid request.

5.10. SUSPENDING AN EXISTING PCL.

a. Upon receipt of a report of adverse information concerning a cleared employee of a contractor, the DoD CAF and DSS will coordinate, as applicable, to obtain such additional information as may be required to determine whether the person's eligibility for access to classified information remains in the interests of national security.

b. Whenever the DSS director has reasonable cause to believe, based on all available facts, that continued access to classified information by an employee of a contractor is not in the interests of national security, the DSS Director is authorized to suspend the DoD NISP collateral clearance eligibility for said contractor employee, after coordination with the DoD Office of the General Counsel. Additionally, the DoD CAF, DSS or other Components, as applicable, may recommend suspension of the DoD NISP collateral clearance eligibility for a contractor employee to the Director, DSS.

b. (Added)(AF) Within DoD, Commanders are not authorized to suspend the collateral clearance eligibility of contractor personnel under the NISP. The Director, DCSA is the sole office delegated authority to make clearance eligibility suspension determinations for NISP contractor personnel. At all times, Commanders retain the authority to make access determinations for contract personnel under the NISP regarding the classified information for which they are responsible in accordance with DoDM 5200.02_AFMAN16-1405. Commanders may also recommend suspension of the clearance eligibility of contractor personnel to the Director, DCSA.

c. Whenever the DSS Director becomes aware of revocation or denial of a contractor

employee's eligibility determination by another adjudication facility, and the DSS Director has reasonable cause to believe that continued access to classified information by that contractor employee is not in the interests of national security, the DSS Director is authorized to suspend collateral eligibility of that contractor employee, after coordination with the DoD Office of the General Counsel. The DoD CAF, DSS or other Components, as applicable, may also recommend to the Director of DSS to suspend the contractor employee's collateral eligibility.

d. In accordance with DoDD 5220.6, the DSS Director is authorized to rescind suspensions made pursuant to Paragraphs 5.10.b and 5.10.c of this volume, after coordination with the DoD Office of the General Counsel, if upon presentation of additional information, the DSS Director determines that continued eligibility for access to classified information is not clearly consistent with the interests of national security.

e. When DSS suspends a DoD NISP collateral eligibility determination for a cleared employee of a contractor, DSS will notify the contractor employee involved concerning the action, the reasons for the action, and provide a copy of the applicable policy issuances. DSS will also notify the employing contractor of the suspension action and request that the contractor remove access for that contractor employee in the DoD personnel security system of record. Under no circumstances will DSS advise the employing contractor of the reasons for the suspension action. If the issue(s) underlying the suspension action could have an impact on the stability of the FCL, DSS will determine what actions are necessary to maintain a valid FCL.

f. The DoD CAF and DSS may disclose information developed in the course of official investigations only to those who have an official requirement for such information. DoD policy strictly prohibits the disclosure of information developed by official investigation to a contractor who is the employer of the subject of the investigation.

g. The GCA will immediately report to DSS any adverse or questionable information that comes to its attention concerning a contractor employee who has been cleared, or is in the process of being cleared, for access to classified information which may indicate that such access is clearly not consistent with the national interest.

g. (Added)(AF) Commanders, program managers, and Information Protection Offices will follow the guidance in paragraph 2.7.h.(1) through 2.7.h.(3) of this volume when making these notifications. (T-1)

h. GCAs issuing access approvals for SAPs or SCI will notify DSS when:

h. (Added)(AF) Air Force security officials responsible for administering access approvals for SAPs or SCI will notify DCSA when taking the actions described in Paragraphs 5.10.h.(1) through 5.10.h.(2) by following the procedures identified in paragraph 2.7.h.(1) through 2.7.h.(3) of this volume. (T-1) If the notification must be made through secure channels, coordinate with the DCSA Special Programs Office.

(1) Taking adverse action on the clearance eligibility or access of a contractor employee or consultant for a contractor with SAP or SCI access.

(2) Becoming aware of any adverse or questionable information concerning a contractor employee or consultant for a contractor with SAP or SCI access.

SECTION 6: CONTRACTING THAT REQUIRES ACCESS TO CLASSIFIED INFORMATION

6.1. GENERAL. A Component and its GCAs will include enough lead-time in the acquisition cycle to accomplish all required security actions. In many instances, advanced planning can ensure that access to classified information will not be required in the pre-award process. This would preclude processing an entire bidder list for FCLs. When access to classified information is not a factor in the pre-award phase, but will be required for contract performance, only the successful bidder or offeror will be processed for an FCL in accordance with Section 4 of this volume.

6.2. PROCEDURES. Before the release or disclosure of classified information to a contractor, the GCA will:

a. Determine the Security Requirements of the Contract

(1) If it is determined that access to classified information will be required in the performance of the contract, the contract is considered to be a "classified contract." When actual knowledge of classified information is not required, but reasonable physical security measures cannot be employed to prevent aural, physical, or visual access to classified information during contract performance, it may be necessary to sponsor an FCL for a company. The GCA or foreign government will indicate such requirement in the DD Form 254 or security aspects letter as applicable. Notices posted to the U.S. Government-wide point-of-entry located at fedbizopps.gov should indicate any FCL requirements. A security requirements clause and a DD Form 254 must be incorporated in the solicitation in accordance with the FAR. Instructions for completing the DD Form 254 are available at www.dss.mil at Job Aids under Professional Education or the Center for Development of Security Excellence. The contractor must possess an FCL at the classification level required for contract performance. Safeguarding capability is required if classified information is to be released to the contractor for possession at its cleared facility.

(1) (Added)(AF) The DD Form 254 Instructions are available at the DoD Directives website at https://www.esd.whs.mil/DD. Air Force personnel will adhere to the DD Form 254 Instructions when preparing the DD Form 254. (T-1)

(a) (Added)(AF) When including security requirements in blocks 10 and 11 of the DD Form 254, the originator will ensure specific guidance is provided in associated comments in block 13, as applicable. (T-1)

(b) (Added)(AF) Originators will identify all places of performance in the DD Form 254. (T-1) If the places of performance may reveal classified information, they may be identified in a classified attachment to the DD Form 254. The originator will include the statement "Reference block 8a-c. See classified attachment" in block 13. (T-1) At a minimum, the originator of the DD Form 254 will include the following in block 8 except

in circumstances where the locations may reveal classified information as described previously: (T-1)

1. (Added)(AF) All contractor facilities where classified performance will occur (i.e., the contractor will store classified material or process classified information at their facility). (T-1)

2. (Added)(AF) The military installation or government facility where classified performance will occur. (T-1) The originator should consider identifying the specific facilities on a military installation where performance will occur (e.g., building number) in block 13 so as to facilitate ease of access for the contractor employees upon commencement of contract performance. Without specific details regarding authorized performance locations, contractors may be denied or delayed access to classified performance locations until the contracting officer or designee can verify the contract requirement and need to know to the organization responsible for the government facility.

(2) If the GCA determines that access to classified information is not required, the contract is not considered a "classified contract" within the meaning of this manual; instead, those are non-NISP contracts that would not require a DD Form 254 or security aspects letter. (See Paragraph 6.2.a.(1) of this volume for those contracts where aural or visual access to classified information cannot be precluded.)

(a) DSS does not fund investigations for non-NISP contracts (i.e., those that do not require access to classified information under DSS security cognizance). GCAs are responsible for funding any and all background investigation requirements established in non-NISP contracts (e.g., network or system administrators, access to government installations or facilities or issuance of the common access card (CAC)). See paragraph 52.204-09 of the FAR and applicable DoD or Component policies for specific guidance. In addition, DSS will not fund an investigative requirement at a higher level than required for access to classified information (e.g., a higher level than required for access to classified information (e.g., a higher level investigation for a system administrator position when access to classified information is only at the SECRET level). The GCA funds the higher level investigation requirement in such cases and upon completion of the investigation, requests the DoD CAF to adjudicate for the applicable clearance eligibility (i.e., for SECRET level clearance eligibility).

(a) (Added)(AF) When a requirement exists for contractor employees to occupy billets designated as national security positions as defined in 5 CFR § 1400, the contracting officer, based on information received from the program manager, will ensure these contractor employees are determined to be trustworthy through the completion of a favorable background investigation commensurate with assigned duties and adjudication by the DoD CAF prior to assumption of sensitive duties. (T-1) Program managers and requirements owners will evaluate the contract performance requirements and inform the contracting officer of the background investigative requirements. (T-1) Designation of these positions is conducted through the use of the Office of Personnel Management Position Designation Tool available at https://www.opm.gov/suitability/suitability-executive-agent/position-designation-tool/. The requirements owner/government sponsor

will identify requirements for contractor background investigations for logical access to government information technology systems, assignment to sensitive duties, or physical access to federal installations. (T-1) The contractor's Facility Security Officer is not responsible for investigation submissions other than those requiring access to classified information. Information Protection Offices will process background investigation requests to the investigative agency for contractor personnel occupying sensitive positions. (T-1) See DoDM 5200.02_AFMAN16-1405, paragraph 5.3.b.(2)(b) for additional guidance.

1. (Added)(AF) In accordance with OUSD(I) Memorandum, *Clarification of Clearance Requirements for Access to Investigative and Adjudicative Relevant Data*, 27 Jun 2019, the investigative requirements for personnel, to include contractor personnel, whose access to military personally identifiable information (PII) or investigative and adjudicative relevant data are as follows:

a. (Added)(AF) Personnel whose access to military PII is limited to data entry or singular search capability require, at a minimum, a favorably adjudicated Tier 1 background investigation. (T-0)

b. (Added)(AF) Personnel whose access to military PII provides the ability to aggregate and extract military PII en masse from an automated records repository require, at a minimum, a favorably adjudicated Tier 3 background investigation. (T-0) Additionally, personnel with routine access to investigative files without the capability to render national security determinations require, at a minimum, a favorably adjudicated Tier 3 background investigation. (T-0)

c. (Added)(AF) Personnel with administrative capabilities in a system storing PII, personnel security investigations, or adjudication determinations require a Tier 5 background investigation. (T-0) Personnel who assess completed investigation files to render national security eligibility determinations or are in positions involving counterintelligence or background investigation duties require a favorably adjudicated Tier 5 background investigation. (T-0)

2. (Added)(AF) Background investigation requirements for access to IT systems are based on the level of access/privileges granted to the user (i.e., IT Level I, II, or III). (T-0) Privileged access is defined in DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, Appendix 1, Definitions, AP1.22. Privileged Access and AFMAN 17-1301, *Computer Security (COMPUSEC)*, Paragraph 4.2.

(b) In instances where a contractor employee requires both a national security determination and a DoD CAC, the eligibility determination to grant access to classified information satisfies the background investigation requirements to support DoD CAC issuance. The DoD CAF will adjudicate the national security investigation at the request of the GCA when clearance eligibility is required.

b. Determine Clearance Status of Prospective Contractors

(1) The GCA will verify the contractor's FCL status and safeguarding capability through the DSS' website. DSS will prominently post instructions at www.dss.mil on how to verify an FCL and safeguarding capability including how to request updates to that information.

(1) (Added)(AF) Contracting officers or designees verify the contractor's FCL status and safeguarding capability by accessing NISS available at www.dcsa.mil. (T-0)

(2) If a facility does not have the appropriate FCL or safeguarding capability, the GCA will submit (i.e., sponsor) a request for an FCL and establishment of safeguarding capability, as applicable, to DSS.

(2) (Added)(AF) The contracting officer or designee will submit a FCL sponsorship request to DCSA electronically through NISS. (T-0)

(3) The lack of an existing FCL is not sufficient justification to exclude a contractor from competing or being awarded a classified contract provided the contractor is willing and eligible to be processed for an FCL and take all required actions associated with such processing on a timely basis.

c. Pre-Award Access to Classified Information

(1) When pre-award access to classified information is required in order for contractors to answer solicitation requirements, the GCA will include information in the pre-award DD Form 254 outlining safeguarding and destruction requirements for the pre-award classified information. Pre-award classified information does not follow the automatic 2 year retention rule as outlined in Paragraph 6.7 of this volume.

(2) GCAs will ensure, prior to issuing pre-award access to classified information, that all prospective contractors have an FCL and safeguarding level that is at least as high as the classification of the pre-award information through the verification process from the DSS website. GCAs will also ensure that any contractor personnel physically receiving pre-award access to classified information have proper courier authorization documents as outlined in DoD 5220.22-M.

(3) When access to classified information is required pre-award, the GCA will inform DSS prior to the solicitation announcement, and provide (at a minimum) the following information:

(a) Solicitation number.

(b) Solicitation release date.

(c) Date solicitation responses are due back to the GCA.

(d) Level of classified involved.

(e) Copy of pre-award DD Form 254, showing requirements for safeguarding and destruction of pre-award classified information.

6.3. SECURITY CLASSIFICATION GUIDANCE.

a. GCAs will ensure that a DD Form 254 is incorporated into each classified solicitation or contract. The GCA will provide the completed DD Form 254 to the prime contractor and to the servicing DSS field office in a timely manner. When preparing classification guidance, the GCA may extract pertinent information from existing security classification guides (SCG) that provide guidance for the classified information that will be furnished to or generated by the contractor. The DD Form 254, with its attachments, supplements, and incorporated references, is the only authorized means for providing security classification guidance to a contractor in connection with a classified contract. It is designed to identify the classified areas of information involved in the classified effort and, particularly, to identify the specific items of information within these areas that require protection. The guidance is provided in the body of the DD Form 254 or its attachments. In the event that the GCA is a foreign government or a NATO activity, a security aspects letter, provided by the foreign government, NATO contracting activity, or Designated Security Authority, serves as the equivalent of a DD Form 254 to provide security classification guidance to a contractor in connection with a classified contract. A security aspects letter assures, in such cases, that the contract includes security requirements for access to classified information if required. In addition, there must be the appropriate foreign disclosure determinations made in accordance with U.S. National Disclosure Policy NDP-1 for access to classified information by the foreign government or NATO activity, as applicable.

a. (Added)(AF) An update or revision to an SCG constitutes a change to security requirements as described in this paragraph and paragraph 3.2.a. of this volume. As a result, the contracting officer must ensure the DD Form 254 is revised and the contract modified for classification changes affecting the contract, to include SCG revisions. (T-0)

b. If the security classification guidance must include classified information, the originator will make an unclassified reference to that information on the DD Form 254 and prepare a classified supplement to the DD Form 254 and forward it by separate correspondence to the contractor and the servicing DSS field office.

c. The GCA will include a DD Form 254 with each request for proposal, inquiry for proposal, or other solicitation and upon award of a contract or follow-on contract to ensure that the facility is aware of the security requirements and can plan accordingly. GCAs are responsible for preparation and execution of the DD Form 254 for prime contracts. The applicable GCA determines whether there are any restrictions or pre-approval requirements for subcontracting (e.g., prior GCA approval to grant access to critical nuclear weapon design information (CNWDI) access to a subcontractor or before any subcontract involving access to intelligence information). While a GCA may receive optional input from the prime contractor for the preparation of classification guidance, the GCA must ensure that such input does not appear to be preselection in the contract award process. A final DD Form 254 will be issued

upon completion or termination of a contract. This DD Form 254 will provide disposition instructions after the automatic 2 year retention period or alternative classified retention guidance.

d. The GCA authorizes and designates USG employees who are knowledgeable of the requirements conveyed in an applicable DD Form 254 (i.e., the contracting officer or designee) to sign on behalf of the GCA. The applicable Component or GCA will ensure that those USG employees designated to sign a DD Form 254 complete appropriate security education and training in accordance with Paragraph 2.7.c of this volume. The GCA will carefully scrutinize requirements requiring higher level access (e.g., TS) given the massive cost differential between PSI types. The GCA will issue a revised DD Form 254 when the security requirements change during the lifetime of the contract.

e. The GCA will provide guidance to the prime contractor for subcontracting. Unless the GCA provides specific contractual direction to the contrary (e.g., access to CNWDI or intelligence information) or DoD 5220.22-M includes a specific requirement, the prime contractor has authority to sign the DD Form 254 for subcontracts.

f. When access to CNWDI is required, the GCA will ensure that the blocks for both RD and CNWDI are marked on the DD Form 254.

g. At least biennially, during classified contract performance, the GCA will conduct a review of the security classification requirements in the DD Form 254.

g. (Added)(AF) Designated GCA personnel will document the review and maintain a record of the review until the next review. (T-1) Records will be maintained with other contract-related documentation. GCA personnel will make this documentation available during self-inspections, Inspector General inspections, etc. (T-1)

h. For guidance with regard to controlled unclassified information, refer to Volume 4 of DoDM 5200.01.

6.4. UNSOLICIATED PROPOSALS. The GCA will use the guidelines in this section when a contractor develops an unsolicited proposal or originates information not in the performance of a GCA contract when such information may be classified.

a. Pursuant to E.O. 13526, information may only be classified if the information is owned by, produced by or for, or is under the control of the USG. The USG cannot classify information over which it has no jurisdiction. The GCA will not classify the proposal or other material unless it incorporates classified information to which the contractor was given prior access or the USG first acquires a proprietary interest.

b. If no prior access was given, the GCA will make or obtain a determination as to whether a classification would be assigned if the USG held a proprietary interest. If the determination is negative, the GCA will advise the contractor that the information is unclassified and any protective marking applied by the contractor is to be removed. If USG proprietary interest is

acquired, the GCA will assign the proper classification after coordination with the cognizant original classification authority (OCA) as required, and notify the contractor.

6.5. PUBLIC DISCLOSURE. The GCA is responsible for and has overall approval authority for the public release of any unclassified information related to the classified contract or subcontract. The procedures of this section also apply to unclassified information pertaining to classified contracts intended for use in unclassified brochures, promotion sales, literature, reports to stockholders, or similar material. The GCA will specify in the DD Form 254 the review procedures for disclosure to the public of all information pertaining to a classified contract.

6.6. CLASSIFICATION INTERPRETATION PROCEDURES. When cleared companies request interpretation from the GCA of the classification guidance furnished to them, or when a contractor believes that information is classified improperly or unnecessarily, that current security considerations warrant upgrading or downgrading of the classification level, or that the guidance is improper or inadequate, the GCA, after coordination with the cognizant OCA as required, will respond to the contractor with corrective action within 60 days. If the GCA has not responded in a timely manner, DSS will provide assistance to the contractor in obtaining a response from the GCA. If the GCA has not responded within 120 days, the contractor may submit a challenge to the Interagency Security Classification Appeals Panel through the ISOO in accordance with E.O. 13526.

6.7. RETENTION OF CLASSIFIED MATERIAL.

a. Unless the GCA provides written instruction to the contrary, contractors are automatically authorized to retain classified information for 2 years upon contract completion in accordance with DoD 5220.22-M.

b. If the GCA wishes to allow retention beyond the automatic 2 year retention period or to permit retention of the classified material in connection with a follow-on or new classified contract, the GCA will provide written authorization to the contractor, by either issuing a final DD Form 254 or a formal authorization letter may also be provided to document the decision.

c. The Component or applicable GCA must assure disposition in accordance with the approved records disposition of the specific Component or GCA supported by the contract effort. As part of its security oversight role, DSS will review contractor records confirming destruction of FGI, upon completion of a contract involving FGI, unless the contract or accompanying security aspects letter, specifically authorizes retention or return of the information to the GCA or foreign government that provided the information.

6.8. DOWNGRADING AND DECLASSIFICATION.

a. The GCA will:

(1) Note on the DD Form 254, or include in attachments thereto, any downgrading or declassification instructions for the information.

(2) Advise the contractor in writing to re-mark the material to reflect the proper designation and to protect it accordingly, if a GCA determines that a contractor has improperly downgraded or declassified information.

(3) Advise the contractor in writing when the contractor is authorized to take actions to declassify or downgrade material because cleared companies are not authorized to unilaterally declassify or downgrade material marked for automatic downgrading or declassification.

(4) Ensure that classified information held by contractors is managed in accordance with their DoD Component records management manuals and identify permanent records of historical value that are subject to automatic declassification. Until such a determination has been made by an appropriate official of the GCA, the classified information contained in such records will not be subject to automatic declassification. The GCA will provide guidance to the contractor that the records will continue to be safeguarded in accordance with the security classification guidance pertaining to the material. For guidance on classification and declassification of permanent records of historical value, refer to Volume 1 of DoDM 5200.01.

(5) Provide classification guidance on identified contracts or programs at cleared companies upon request by DSS.

b. DSS will contact the appropriate GCA and request that guidance be provided to the contractor when notified by a contractor that adequate security classification guidance has not been provided.

SECTION 7: SAFEGUARDING

7.1. GENERAL. DoD 5220.22-M establishes baseline requirements for contractor safeguarding of classified information. DoD 5220.22-M does not require accountability for SECRET or CONFIDENTIAL information by the contractors. DoD information security policy to protect classified information is contained in DoDI 5200.01 and Volume 3 of DoDM 5200.01. These DoD policy issuances implement E.O. 13526.

7.1. (Added)(AF) Information Protection Offices will follow the guidance in DoD 5220.22-M when evaluating and approving safeguarding of classified information for on-installation cleared facilities. Information Protection Offices will follow the guidance in AFI 16-1404, when evaluating and approving safeguarding of classified information for visitor groups.

7.2. STORAGE OF CLASSIFIED MATERIAL.

a. Part 2001 of Title 32, CFR sets forth the requirements for the safeguarding of classified national security information for all USG agencies. Classified information must be stored only under conditions designed to deter and detect unauthorized access to the information in accordance with Part 2001 of Title 32, CFR. DoD 5220.22-M describes the uniform requirement for the physical protection of classified material in the custody of contractors. DSS may approve compensatory provisions for the storage of classified material where the requirements of DoD 5220.22-M are not appropriate for protecting specific types or forms of classified material. See Paragraph 2.2.x of this volume.

a. (Added)(AF) The Installation Commander may approve compensatory provisions for the storage of classified material in on-installation cleared facilities where the requirements of DoD 5220.22-M are not appropriate for protecting specific types or forms of classified material in accordance with Paragraph 2.2.x. of this volume.

b. DoD 5220.22-M specifies supplemental protection measures to be used by a contractor.

c. DSS will, when acting as the CSO:

c. (Added)(AF) When the Installation Commander provides oversight of on-installation cleared facilities, the Information Protection Office will (T-1):

(1) Approve container storage capability prior to contractor receipt of classified information. Approve collateral closed areas or vaults prior to use for storage of classified information. DSS may delegate approval authority for additional closed areas or vaults to contractor personnel who meet specified qualification criteria established by DSS. DSS always retains oversight and ultimate approval authority.

(1) (Added)(AF) Installation Commanders will not delegate approval authority for additional closed areas or vaults to contractor personnel. (T-1) The Information Protection Office, operating under the authority of the Installation Commander, will issue

approvals for additional closed areas or vaults to contractor personnel. (T-1)

(2) Approve or disapprove contractor requests for open shelf or bin storage of classified documents in closed areas in accordance with DoD 5220.22-M. Open shelf or bin storage by contractors for TS information is not permitted.

(3) Determine the supplemental protection measures that may be used by the contractor and inspected by DSS, after considering the classification level and nature of the material to be protected as well as the storage method used and other relevant circumstances.

(a) Provide criteria to its personnel to use in determining whether a contractor's security in depth plan is sufficient. The criteria will foster consistency in DSS decisions as to the acceptability of a contractor's security in depth plan with any supplemental protection measures implemented by the contractor. DSS will also advise the GCAs that have classified contracts at a contractor facility when DSS considers the location to have security-in-depth.

(b) When appropriate, DSS will approve the installation and use of an intrusion detection system that meets the criteria of ICD 705, Underwriter Laboratories Standard 2050, or an equivalent system approved by the CSA in writing, when supplemental protection is required by DoD 5220.22-M for the storage of SECRET and TS material.

7.3. TRANSMISSION OF CLASSIFIED INFORMATION.

a. TS classified information may be transmitted provided the following conditions are met:

(1) The GCA must provide written approval to the contractor before TS material can be transmitted outside of a contractor facility.

(2) The GCA must provide written approval before a contractor can use the U.S. Transportation Command's Defense Courier Division (TCJ3-C)).

(3) The GCA must provide written approval if a contractor wants to use approved secured COMSEC circuits.

b. SECRET or CONFIDENTIAL material may be transmitted provided the following conditions are met:

b. (Added)(AF) When the Installation Commander provides oversight of an on-installation cleared facility, the Information Protection Office will perform government responsibilities otherwise assigned to DCSA regarding transportation of SECRET or CONFIDENTIAL material. (T-1)

(1) The GCA will provide written direction for the transmission of SECRET or CONFIDENTIAL material if the methods specified for SECRET transmission in DoD 5220.22-M cannot be used.

(2) DSS may approve the use of a commercial delivery company for overnight transmission of SECRET or CONFIDENTIAL material by a contractor in accordance with Part 2001 of Title 32, CFR, provided the commercial delivery company:

(a) Is a current holder of the General Services Administration (GSA) contract for overnight delivery within the United States and its territories for the Executive Branch (a list of the current contract holders under Multiple Award Schedule 48, "Transportation, Delivery and Relocation Solutions," is posted at www.gsa.gov).

(b) Provides nationwide, overnight service with automated in-transit tracking of the classified material.

(c) Ensures package integrity during transit.

(d) Is U.S. owned and operated.

(3) Commercial delivery companies may not be used for COMSEC, NATO, or FGI in accordance with Part 2001 of Title 32, CFR.

(4) DSS will approve contractor procedures prior to use of a commercial delivery company which is to ensure the proper protection of classified packages transmitted by such means and that incoming shipments are received by appropriately cleared contractor personnel.

(5) If DSS authorizes a contractor to receive SECRET and CONFIDENTIAL material via a GSA commercial delivery company, DSS will record a street delivery address for this purpose. DSS will make this information available to GCAs and other cleared companies that are authorized transmission of SECRET and CONFIDENTIAL material via GSA commercial delivery companies. Prior to transmission of classified material, the GCA will verify with DSS that a contractor has an approved street delivery address. Verification of a contractor's approved street delivery address as an authorized overnight delivery address indicates approval of the receiving contractor's ability to receive classified material.

(5) (Added)(AF) When the Installation Commander retains oversight of on-installation cleared facilities, the servicing Information Protection Office will provide DCSA the classified mailing address for the cleared facility for entry into the system of record. (T-1)

c. If the transmission methods specified in DoD 5220.22-M cannot be used, the GCA will provide written authorization in accordance with the provisions of Section 12 of this volume for the transmission of classified material to a USG activity outside the United States or a U.S. territorial area, if the contract does not already provide for such transmission.

d. The Defense Transportation System (DTS) is generally used for the transportation of classified material. If DTS resources are unavailable or if using DTS is cost prohibitive, a commercial carrier may be used in accordance with the procedures in DoD 5220.22-M and

DoD 4500.9-R.

7.4. REPRODUCTION OF CLASSIFIED MATERIAL.

a. DoD 5220.22-M requires that contractors establish a reproduction control system to ensure that reproduction of classified material is held to the minimum consistent with contractual and operational requirements. TS material may be reproduced only as necessary in the preparation and delivery of a contract deliverable. SECRET and CONFIDENTIAL material may be reproduced as necessary for performance of a prime or subcontract; in preparation of solicited or unsolicited bid, quotation, or proposal; or for preparation of patent applications to be filed in the U.S. Patent Office. See Paragraph 4.8.c.(14)(c) of this volume and Paragraph 12.19.b.(2) of this volume for additional guidance on patent attorneys or patent firms.

b. The Component or GCA will:

(1) Serve as the approval authority for the reproduction of TS material by a contractor for any reason other than as necessary in the preparation and delivery of a contract deliverable.

(2) Indicate in the DD Form 254 if special conditions exist to warrant the restriction of the reproduction of SECRET or CONFIDENTIAL material beyond the criteria of DoD 5220.22- M.

7.5. DESTRUCTION OF CLASSIFIED MATERIAL.

a. DoD 5220.22-M authorizes the methods that contractors may use to destroy classified material in their possession when it has served the purpose for which it was released by the USG, developed or prepared by the contractor, or retained after completion of termination of a classified contract. See Paragraph 4.8.c.(11) of this volume for FCL requirements for commercial destruction facilities. DSS must approve any methods of destruction of classified material, to include any classified hard drives, not specifically authorized in DoD 5220.22-M. DSS must also approve the conditions and use of public destruction facilities for classified material.

a. (Added)(AF) When the Installation Commander provides oversight of on-installation cleared facilities, the Information Protection Office will approve methods of destruction for the cleared facility. (T-1)

b. The GCA will indicate in the DD Form 254 if special conditions exist to warrant the execution of a signed destruction certificate when destroying SECRET material.

SECTION 8: INQUIRIES, INVESTIGATIONS, AND ADMINISTRATIVE ACTIONS

8.1. APPLICATION. This section establishes the procedures for the conduct of administrative inquiries, investigations, and administrative actions based on contractor reporting.

8.2. PROCEDURES FOR SUSPICIOUS CONTACTS, POSSIBLE ESPIONAGE, SABOTAGE, ACTS OF TERRORISM, OR SUBVERSIVE ACTIVITIES.

a. DSS will support contractors consistent with DoD 5220.22-M, DoDD 5105.42, and also DoDD 5240.06 if required by contract, in the:

(1) Recognition and reporting of suspicious contacts.

(2) Reporting of foreign intelligence entity threats in accordance with DoDD 5240.06, and Section 3381 of Title 50 U.S.C.

b. DSS will:

b. (Added)(AF) For on-installation cleared facilities or contractor visitor groups, the Installation Commander or designee will (T-0):

(1) Forward information received from any source involving espionage, sabotage, terrorism, or subversive activities or any case that involves RD or FRD, and the possibility that a criminal violation of Section 2011 of Title 42, U.S.C. has occurred involving a contractor or contractor employees to the Federal Bureau of Investigation (FBI). DSS forwards the information to the FBI consistent with the August 2, 2011 FBI DoD Memorandum of Understanding (MOU).

(a) DSS will notify the Defense Intelligence Agency (DIA) and the appropriate Military Department Counterintelligence Organization (MDCO) at the same time that DSS forwards the information to the FBI when the allegations described in Paragraph 8.2.b of this volume potentially involve a Component's equities or a DoD affiliated individual as defined in the August 2, 2011 FBI DoD MOU.

(b) DSS will keep DIA apprised of any updates provided by the FBI with FBI's permission. Once information referred to the FBI or an MDCO has been accepted for investigation, planned, ongoing, or previous CI activities conducted by or in support of the FBI or MDCO may not be disclosed without specific authorization from the FBI or MDCO.

(2) If the FBI or an MDCO opens an investigation, DSS will defer any other investigative actions until authorized by the FBI or MDCO. Any action DSS desires to take relative to NISP requirements will be closely coordinated in advance with the FBI or the MDCO before DSS takes any such action.

(3) If DSS learns of additional information believed to be of interest to the FBI or the MDCO involved, DSS will furnish that information as soon as possible.

(4) When DSS learns of the final disposition of the case, DSS will advise DIA of the outcome after receiving permission of the investigating organization.

(5) DSS will request periodic updates from the investigating organization on investigations or other actions that require DSS take action under its NISP oversight responsibilities. DSS will request updates to occur every 90 days.

c. The Component will advise DSS, after coordination with the FBI, of any contractor or contractor employees known or suspected to be involved in possible espionage, sabotage, terrorism, or subversive activities.

d. DSS will not initiate CI inquiries into contractor facilities or activities but will refer suspicious contacts and information regarding possible espionage to the FBI, the MDCOs, or other federal CI or law enforcement entities as required for appropriate action.

8.3. LOSS, COMPROMISE, OR SUSPECTED COMPROMISE OF CLASSIFIED INFORMATION.

a. Upon identification or notification from or by a contractor as required by DoD 5220.22-M of a loss, compromise, or suspected compromise of classified information, DSS will provide an initial notification to the applicable security manager at the Component or its affected GCA and will provide notification to the FBI, MDCOs, and Defense Criminal Investigative Service, or the Director, OUSD(I) CI&S, in accordance with the provisions of Volume 3 of DoDM 5200.01 and Section 3381 of Title 50, CFR.

a. (Added)(AF) When the Installation Commander provides oversight of an on-installation cleared facility, the Information Protection Office will conduct the actions required of DCSA in Paragraphs 8.3.a. through 8.3.i. except where identified otherwise. (T-1)

b. Upon receipt of a preliminary report involving loss, compromise, or suspected compromise of classified information, DSS will:

(1) Take immediate steps to ensure that the contractor establishes and implements adequate safeguards if the report determines additional classified information, other than what is known or suspected of being compromised, may also be in danger of being compromised due to poor security practices or procedures. Such steps may involve an immediate visit to the contractor.

(2) Establish a deadline for the contractor to submit a final report if the preliminary report does not contain sufficient detail to reach a final determination that a loss, compromise, or suspected compromise occurred.

(3) Immediately ensure that the cleared facility is in compliance with the provisions of its DSS-approved plan if the preliminary report deals with a spillage of classified information (i.e., onto an unclassified IS, or higher level classified information onto a lower level classified IS or onto an IS not accredited to the appropriate level). The applicable security manager for the Component or affected GCA will advise DSS if, in consultation with the OCA, if more stringent measures are required than those described in Section 11 of this volume.

(3) (Added)(AF) When the Installation Commander retains oversight of on-installation cleared facilities, the supporting Cybersecurity Squadron will ensure the required actions are taken to mitigate the effects of a spillage of classified information as described in this paragraph. (T-1)

(4) Forward the report within 24 hours of receipt to the SDDC if the preliminary report deals with classified shipments in transit by a commercial carrier.

(5) Refer any inquiries about the security incident with the applicable security manager for the Component and the affected GCA.

(6) Advise the contractor that no further investigation or report is required and consider the report to be final if the preliminary report contains sufficient details to make a final determination in the case.

c. Upon receipt of the contractor's final report, DSS will:

(1) Review the report for adequacy and assess CI significance for analysis and coordination with DSS CI and sharing with the appropriate CI element in accordance with Paragraph 8.2 of this volume.

(1) (Added)(AF) When the Installation Commander maintains oversight of on-installation cleared facilities, the supporting AFOSI detachment will take the actions required to assess the report for counterintelligence significance. (T-1)

(2) Conduct additional inquiry, if necessary to obtain all of the facts pertaining to the incident.

(3) Make a final determination as to whether or not a loss or compromise occurred.

d. DSS will ensure that the contractor has taken adequate action to prevent incidents that could lead to future losses or compromises if it is determined that a loss, compromise, or suspected compromise did not occur.

e. DSS will provide a report to the affected Component and appropriate GCA if a determination is made that a loss, compromise, or suspected compromise has occurred so that the affected Component and the appropriate GCA can take the necessary steps in accordance with the provisions of Enclosure 6 of Volume 3 of DoDM 5200.01. The report will contain:

e. (Added)(AF) When the Installation Commander provides oversight of on-installation cleared facilities, the Information Protection Office will route the final report of security violation to DCSA through MAJCOM information protection channels and will enter the report into the SAF/AAZ designated repository. (T-1)

(1) Authority. Cite the reason for the inquiry including when, where, and who conducted it.

(2) Essential Facts. Fully identify the information involved and arrange the relevant factually-based events (not opinions or assumptions) in chronological order. If available, provide the contract number associated with the classified information. Conflicting assertions of fact should also be discussed.

(3) Corrective Action. Specify action taken to preclude a recurrence of similar incidents and the disciplinary action, if any, taken against responsible individual(s).

(4) Conclusions. Summarize conclusions reached as a result of the facts, and provide an analysis of all pertinent information. Conclusions should follow the sequence of reported facts. Provide a rationale if conclusions differ from the contractor's conclusions.

(5) Recommendations. Include, as applicable, any proposed actions that could affect disposal of the case by the affected Component, OCA and appropriate GCA. The recommendations should be consistent with the conclusions.

(6) Attachments. Include a copy of the contractor's report of inquiry with the identification of specific individuals redacted. If the contractor's report contains sufficient detail, DSS may supplement the report rather than duplicating the contractor's conclusions.

f. DSS will make a determination as to whether a weakness in security practices or procedures caused or permitted the loss, compromise, or suspected compromise, and ensure that such practices and procedures are corrected.

g. DSS will consider recommending suspension of an individual's PCL in accordance with Section 5 of this volume if it is determined that an individual caused the loss, compromise, or suspected compromise and the individual's actions were egregious or a part of a pattern of security violations.

h. After the applicable Component and OCA receive the report or notification that a compromise has occurred, the OCA will take the actions required by Enclosure 6 of Volume 3 of DoDM 5200.01 and advise DSS of the results.

i. In the case of lost TS classified material, DSS will make a determination as to whether the contractor's accountability for the TS item(s) should be terminated. If an adequate and exhaustive search has been made, and additional effort would not be expected to lead to the recovery of the material or provide a probable explanation of the manner of loss, DSS will

direct the contractor to terminate accountability for the lost TS material. An information copy of the letter directing termination of accountability of the TS material must be forwarded to the OCA and the applicable Component. The Component should be notified if the contractor subsequently locates or recovers the item. If COMSEC material is involved, DSS will notify the NSA/CSS.

8.4 COMPONENT OR GCA REPORTING. A Commander or his designee will provide DSS with information regarding any suspicious contacts or other incidents related to on-site contractors in accordance with the provisions of this section and Section 8 of this volume. The Commander's notification will occur within 72 hours of knowledge of the incident's occurrence and also be provided to the contractor's FSO. Such reporting would include data spills of classified information by contractors on the Component or affected GCA's IS. If the Commander has identified a culpable contractor employee for a security incident, he will submit an incident report via the DoD personnel security system of record.

8.4. (Added)(AF) Commanders will provide such notifications through their servicing Information Protection Office. (T-1)

8.5 RESPONSIBILITY OF THE COMPONENT AND GCA TO INVESTIGATE CERTAIN BREACHES OF SECURITY. When an unauthorized public disclosure of classified information is discovered and it is not possible to determine whether it emanated from a USG or contractor source, the applicable Component or affected GCA will promptly initiate an investigation of the breach in order to determine the cause and establish responsibility in accordance with Volume 3 of DoDM 5200.01. The applicable Component or affected GCA will:

8.5. (Added)(AF) Air Force personnel will follow the guidance in AFI 16-1404, when conducting these investigations. (T-1)

a. Ensure adequate corrective action is taken to prevent future compromise of this nature if a USG source is determined to be responsible.

b. Provide DSS with all information related to the GCA sponsored investigation to include written reports of culpability, if available, and request that DSS take appropriate action if it is determined a contractor, its employees or consultants are responsible. This information should include:

b. (Added)(AF) The information provided to DCSA need only contain information related to cleared contractors involved in the investigation. Otherwise, Air Force personnel will adhere to the requirements for such investigations as described in AFI 16-1404. (T-1)

(1) Recommending the revocation or suspension of PCLs of contractor employees involved in the security breach, if warranted.

(2) Informing the contractor of the corrective action that must be taken to prevent future

compromises of this nature.

c. Comply with the provisions of Enclosure 6 of Volume 3 of DoDM 5200.01 in the reporting and notification of security incidents involving classified information.

SECTION 9: SETA

9.1. APPLICATION. This section describes the SETA aspects of the NISP and outlines its scope and operation. DSS and GCAs use SETA to:

a. Inform contractors of the requirements of DoD 5220.22-M for the NISP, the principles of industrial security; alert them to the dangers of espionage and sabotage as well as actual or potential insider threat; and suggest preventative measures that cleared companies may adopt to avoid such dangers.

b. Acquaint GCA personnel with the requirements of the NISP and this manual; the principles of industrial security; and with the philosophies, requirements, and techniques embodied in the NISP.

9.2. SETA

a. In accordance with DoDI 3305.13, DSS serves as the functional manager responsible for the execution and maintenance of DoD security training and appoints the chair of the DoD Security Training Council.

b. DSS will:

b. (Added)(AF) When the Installation Commander provides oversight of on-installation cleared facilities, the Information Protection Office will perform the responsibilities in Paragraphs 9.2.b.(7) and 9.2.b.(8). (T-1)

(1) In accordance with DoDD 5105.42, develop, maintain, and administer security education and training products and services. For the industrial security discipline, the effort will include establishing training programs as deemed appropriate, conducting security education and training, providing professional development support services, and preparing and distributing information and technical guidance materials for contractor and Component personnel (including industrial security professionals and contracting officer representatives). The program will include threat awareness security information as well as CI and insider threat awareness information.

(2) Train Component personnel and others performing security duties (e.g., contracting officer representatives or personnel serving as a designated government representative) on the requirements of this manual and of industrial security matters upon request.

(3) In concert with the guidance in DoD 5220.22-M, determine the industrial security education and training requirements of contractor employees or consultants informing them of the availability of education and training materials and providing advice and guidance on industrial security education and training matters.

(4) Leverage training available from other USG sources, industry, and educational

institutions to augment the DSS training capacity, provided the other sources concur with DSS usage. DSS can also partner with professional organizations and industry groups to provide security education, training, and support functions to contractor employees or consultants as appropriate.

(5) Prepare appropriate material for dissemination in execution of this program with input from Components and contractors.

(6) Develop qualification criteria and training programs for contractors to meet prior to granting self-approval authority for such areas including, but not limited to, controlled areas, classified storage or destruction of classified material. DSS should accept training and expertise gained by contractor personnel from other sources including USG agencies, professional organizations, and educational institutions when assessing a contractor's qualification for self-approval authority.

(7) Verify during oversight visits that the U.S. contractor provides security education and awareness training for cleared employees assigned outside the United States, a responsibility of the U.S. contractor, as specified in DoD 5220.22-M.

(8) Provide initial security briefings to contractor FSOs and ensure that other briefings required for special categories of information are provided to contractor personnel.

SECTION 10: VISITS AND MEETINGS

10.1. GENERAL

a. This section establishes procedures and responsibilities regarding visits to USG activities and contractor facilities where access to classified information is involved. Authorized and credentialed representatives of DoD, DSS, other GCAs, auditors, and representatives of USG investigative agencies, to include officially credentialed contract investigative providers, are not considered to be visitors under this section when acting on behalf of the USG in their official capacities.

b. Classified information may be disclosed during visits if the visitors possess appropriate PCLs and have a valid need-to-know for the classified information. The responsibility for determining need-to-know lies with the individual who discloses classified information during a visit. Consistent with DoD 5220.22-M, need-to-know is generally based on a contractual relationship. In other circumstances, disclosure of the information will be based on an assessment that the receiving contractor or its cleared employees have a bona fide need to access the information in furtherance of a GCA purpose.

c. Foreign visits to U.S. Government and contractor facilities involving access to classified information are governed by DoDD 5230.20 as referenced in Paragraph 12.16.a of this volume. Contractors under the NISP must comply with DoD 5220.22-M.

10.2. VISITS TO CONTRACTOR FACILITIES

a. If a visit to a contractor facility requires access to classified information, the visitor's PCL level, special access authorization, citizenship, purpose of the visit, etc., must be verified by the host contractor in accordance with DoD 5220.22-M. Verification by DoD Components or their GCAs may be accomplished by review of Joint Personnel Adjudication System (JPAS) or the successor DoD personnel security system of record for eligibility and access information that contains the clearance information or by a visit authorization letter (VAL) provided by the visitor's employer. Non-DoD Components and their GCAs will accomplish such a verification through the Central Verification System of the Office of Personnel Management or by a visit authorization letter (VAL) provided by the visitor's employer.

b. Procedures must be in place to ensure positive identification of visitors prior to disclosure of classified information.

10.3. VISITS TO USG ACTIVITIES BY CONTRACTOR PERSONNEL

a. GCAs will verify that the visitor's employing company has an FCL through ISFD. Once a company's FCL is established, the hosting DoD Component or GCA will review JPAS or the successor DoD system of record for eligibility and access information to determine the PCL of

the visiting contractor employee. Non-DoD Components and their GCAs will review the Central Verification System of the Office of Personnel Management for eligibility and access information to determine the PCL of the visiting contractor employee. If the hosting USG activity does not have access to the applicable database, the hosting USG activity will rely on the employing contractor's VAL certifying the clearance of their employee; and will also take steps to gain access to the applicable database to determine the PCL of future visiting contractor employees. When the contractor attempts to visit a USG activity without prior notice to the GCA host activity, the GCA may request additional detail or justification from the contractor to determine whether to accept the visit and provide access to classified information.

a. (Added)(AF) Air Force activities will verify that the visitor's employing company has an FCL through NISS. (T-0)

b. Visits to USG activities located outside of the United States will be processed in the same manner as other classified visits.

10.4. MEETINGS AT WHICH CLASSIFIED INFORMATION IS DISCLOSED. Volume 3 of DoDM 5200.02 provides specific DoD requirements regarding classified meetings, including provisions for an exception to policy with regard to the location of the classified meeting. DoD 5220.22-M provides similar requirements to contractors for classified meetings.

10.4. (Added)(AF) Volume 3 of DoDM 5200.01, *DoD Information Security Program: Protection of Classified Information*, along with AFI 16-1404, provide specific DoD requirements regarding classified meetings, including provisions for an exception to policy with regard to the location of the classified meeting.

SECTION 11: IS SECURITY

11.1. GENERAL. IS that are used in the collection, processing, storage, transmission, display, dissemination, and disposition, of classified information must be properly managed to protect against unauthorized disclosure of classified information and, if required by contract, the loss of the availability and integrity of the information and the system. DoD 5220.22-M addresses the baseline protection standards for classified information applicable to contractors. This section provides the IS security procedures for:

a. DSS as the CSO and AO for contractor IS processing classified information in accordance with DoDD 5105.42.

a. (Added)(AF) When Installation Commanders provide oversight of on-installation cleared facilities, the authorizing official for information systems processing classified information in these contractor facilities is the Air Force appointed authorizing official. These systems are authorized as government systems which differs from how DCSA authorizes systems at contractor facilities. The supporting cybersecurity squadron must provide information system support and oversight for classified information system requirements at on-installation cleared facilities. (T-1)

b. GCAs with procurement requirements for contractors to process classified information on IS or connect to a GCA network.

b. **(Added)(AF) These information systems security procedures apply when the Air Force desires to install federal information systems under Air Force authorization in cleared contractor facilities under oversight by DCSA.**

11.2. DSS. In accordance with Section 2 of this volume, DSS, as the AO, will:

a. Authorize contractor's IS located in the contractor's cleared facility(ies), to process classified information in accordance with the criteria in DoD 5220.22-M. The underlying principles in DoD 5220.22-M for assessment and authorization of contractor IS are those established in the Committee on National Security Systems (CNSS) requirements as noted in CNSS Policy (CNSSP) 22, CNSS Instruction (CNSSI) 1253, and National Institute of Technology and Standards Special Publication 800-37 guidelines. These risk management principles incorporate security controls into the system from its concept stage through its life cycle. They provide for continuous risk assessment and monitoring, vulnerability and incident management, the application of best security practices and conservation of resources to ensure security risk is maintained at acceptable levels.

b. Develop, issue, and update (as necessary):

(1) Implementation and process guidelines and technical standards to contractors in support of DoD 5220.22-M.

(2) Templates to facilitate IS security and the authorization process for contractors.

(3) MOU examples and templates to facilitate the connection of contractor IS to systems authorized by other AOs. GCAs are encouraged to use these MOU examples and templates.

(4) A "notice and consent" approved banner for use by contractors on approved IS to notify users that:

(a) System usage is monitored, recorded, and subject to audit.

(b) The user has consented to such monitoring and recording by using the system.

c. Provide authorization specifically in writing to a contractor when a contractor information system security manager may extend an existing authorization to similar systems within parameters specified by DSS.

d. Execute MOUs, when requested, to allow for connection of authorized contractor IS to networks on systems authorized by other AOs. MOUs are not to be established that limit or change DSS cognizance responsibilities or security controls required by DoD 5220.22-M.

e. Ensure, in accordance with CNSSP 18 that all contractors under DSS cognizance have a plan in place for dealing with classified information spills on IS, whether the contractor has authorized systems or not. When requested, DSS will provide approved procedures to contractors to meet this requirement.

(1) The DSS-approved procedures are intended for use on contaminations involving information at or below the TS collateral level unless directed by the GCA to follow more stringent measures. DSS will approve any facility-specific changes or use of a different plan in writing.

(2) DSS will verify that the contractor has taken mitigation actions, including disposition of affected media (e.g., sanitization, physical removal, or destruction), in accordance with decisions by the GCA in consultation with the information owner, if the GCA requires more stringent measures as noted in Section 8 of this volume.

f. Assess the effectiveness of IS security controls as implemented by the contractor through on-site validation and inspection. Advise contractor management and, as warranted, the GCA if controls are not implemented correctly or effectively. Ensure that required corrective actions are implemented by the contractor on a timely basis.

11.3. GCA. A GCA having a contract requiring a contractor IS to process classified information, or to connect to a classified network for contract performance:

a. May direct a contractor to perform a risk assessment to determine if additional countermeasures beyond those identified in DoD 5220.22-M are required or if an identified

unique local threat exists. In either instance, the GCA will provide the local DSS field office with a copy of the contractor's completed risk assessment and coordinate with DSS on the contractor's application of any additional agreed upon countermeasures beyond the standards in DoD 5220.22-M. A risk assessment does not authorize a GCA to weaken or downgrade security controls required by this manual.

a. (Added)(AF) An Air Force GCA who directs a contractor to perform a risk assessment to determine if additional countermeasures beyond those identified in DoD 5220.22-M are required or if an identified unique local threat exists must communicate such a requirement through the contract. (T-1)

b. Will identify if there is a need and provide guidance to the contractor regarding additional security requirements for incident and vulnerability management (scanning and remediation and reporting procedures) that exceed DoD 5220.22-M standards and baseline technology security configurations for the IS. In those instances, the GCA will provide the local DSS field office with a copy of any such guidance provided to the contractor.

b. (Added)(AF) An Air Force GCA who identifies there are additional security requirements for incident and vulnerability management (scanning and remediation reporting procedures) that exceed DoD 5220.22-M standards and baseline technology security configurations for the information system will provide such guidance to the contractor through the contract. (T-1)

c. Will issue additional written guidance or requirements to the contractor if there is a contractually mandated requirement for data integrity or system availability controls above the requirements in DoD 5220.22-M and provide DSS with a copy of any such guidance provided to the contractor.

d. Will determine if a contractor IS processing classified information is a special category system and include in the applicable DD Form 254 the security requirements for said contractor IS.

(1) If the GCA has determined the contractor IS to be a special category system, the GCA must assess and, if requested by DSS, endorse any contractor proposed alternative controls submitted to DSS.

(2) If the GCA has not provided the security requirements for tactical, embedded IS described in DoD 5220.22-M, the contractor will request them from the GCA. If the GCA does not then provide the security requirements as requested by the contractor, DoD 5220.22-M requires the contractor to submit classified processing procedures to DSS that describe the security requirements and procedures implemented that protect the embedded system and classified information against unauthorized disclosure or loss.

e. Will, in consultation with the applicable information owner, provide the contractor, with a copy to DSS, written guidance and direction to be used regarding mitigation procedures in the event of an electronic data spillage of classified information onto an unclassified IS, or higher

level classified information onto a lower level classified IS or onto an IS not accredited to the appropriate level.

f. May certify in contract documentation why a contractor is unable to comply with the CSA provided security control baseline due to operational requirements or added cost to the program. The contract documentation may be:

(1) In the DD Form 254, formal classification guidance or a formal memorandum signed by the contracting officer, the contracting officer's representative or the Government Program Manager that clearly cites one or more of the circumstances noted in Paragraphs 11.3.f.(2)(b)(1) through 11.3.f.(2)(b)(3) of this volume and must be provided to DSS. A formal contract modification is not necessary.

(2) The documentation or written statement should include rationale for the decision.

(a) The statement must be signed by the contracting officer, the contracting officer's representative or the contracting officer's technical representative, or the Government Program Manager. A formal contract modification is not necessary.

(b) The written statement should include rationale such as:

1. The contractor is required to use an operating system (OS) (identify the OS) that is not capable of meeting, audit requirements in DoD 5220.22-M;

2. Enabling auditing on a legacy OS will result in unnecessary costs, operational impacts, or deviation from the secure deployed operating environment; or,

3. The IS, determined to be a special category system, meets the requirements of DoD 5220.22-M and can be adequately secured without all of the DoD 5220.22-M technical requirements being implemented.

g. May provide, when requested by DSS or the contractor as part of the ATO process, its formal acknowledgement of the associated risk to the classified information when it is not feasible for contractors to implement the CSA provided security control baseline due to operational requirements or added cost to the program.

h. Will provide a signed letter acknowledging risk acceptance or security oversight for a contractor CSA-authorized mobile system or contractor mobile restricted or mobile closed area containing CSA-authorized mobile system, prior to a contractor relocating the system to a USG activity or commercial test site (i.e., aircraft or satellites during ground movements, aerial test flights or launches).

i. Will require the establishment of an MOU to document the terms and conditions for sharing data and information resources in a secure manner when there is a need for connection to a USG system. Specifically, the MOU defines the purpose of the interconnection; identifies relevant authorities; specifies the responsibilities of both organizations and network

participants; and defines the terms of agreement and the timeline for terminating or reauthorizing the interconnection. The MOU should not include technical details on how the interconnection is established or maintained; that is the function of the Interconnection Security Agreement (or Network Security Profile).

j. Will, when notified of a classified information spill by a contractor, and in consultation with the applicable information owner, provide the contractor in writing its concurrence with the DSS-approved plan or notice of more stringent measures to be used for mitigation procedures. Clean-up procedures may be approved by the GCA in advance to facilitate prompt clean-up.

j. (Added)(AF) The Information Protection Office will ensure a copy of the written concurrence regarding clean-up procedures is provided to SAF/AAZ. (T-1)

k. Will provide the authority and guidance in the DD Form 254 if masking, coding, or disassociation to disguise classified information by any prime or sub-contractors required to be used. In some instances techniques such as “masking,” “coding,” or “disassociation” may be used to disguise an item of classified information. If all classified information to be processed is disguised by one of these methods, the IS does not require accreditation by DSS.

11.4. FEDERAL IS OPERATING IN CONTRACTOR CLEARED FACILITIES.

a. Components and their GCAs will ensure that when they require federal IS processing classified information to operate in contractor cleared facilities, they document the requirement in a formal agreement with the contractor. The formal agreement will require that the federal IS be in an area designated as government space, with physical separation (e.g., office, room or building) from other contractor operations and be clearly identified for DSS and the Component or applicable GCA to prevent confusion regarding oversight responsibilities. DSS does not have oversight or AO responsibility for federal IS operating within a designated government space within a contractor-cleared facility.

b. If a Component or GCA needs to locate a federal IS at a contractor cleared facility that does not meet the criteria of Paragraph 11.4.a of this volume, the Component or GCA will request an exception for consideration by DSS in accordance with the provisions of Paragraphs 2.2.x and 3.3.a of this volume.

SECTION 12: INTERNATIONAL SECURITY PROGRAMS

12.1. GENERAL. This section provides the requirements and procedures for the protection of U.S. classified information and FGI (including NATO information) to which U.S. contractors may have access as the result of contracts, subcontracts, pre-contract negotiations, agreements, and other programs or projects involving foreign governments and foreign companies. All such initiatives are international programs for the purpose of this manual. They may be related to direct commercial sales (DCS), foreign military sales (FMS), or other international initiatives involving a U.S. contractor and a foreign government or foreign contractor under which classified information is provided, generated, or transferred. International security requirements levied on U.S. contractors are in DoD 5220.22-M.

12.1. (Added)(AF) When the Installation Commander provides oversight of on-installation cleared facilities, the Information Protection Office will maintain a working relationship with the supporting foreign disclosure office, the DCSA field office in the geographic area of the installation, and the international division at Headquarters DCSA, to ensure responsibilities regarding Section 12 of this volume are adequately covered. (T-1) In general, the Information Protection Office performs the responsibilities assigned to DCSA in Section 12 but may require assistance from DCSA as the CSO to complete all tasks.

12.2. AUTHORITY FOR INTERNATIONAL PROGRAM SECURITY REQUIREMENTS. The security requirements for international programs are derived from the ITAR, for export and import of defense articles and defense services; DoDD 5230.11 for proposed disclosures of classified military information to foreign governments; bilateral security agreements and program-specific agreements with allies and other friendly countries; and the NATO requirements implemented by United States Security Authority for NATO Affairs Instruction 1-07, as described in DoD 5220.22-M.

a. DSS will exercise oversight of U.S. contractor security arrangements for exports of classified defense articles and technical data in accordance with DoDD 5201.42 to ensure that exports of classified defense articles and technical data are in compliance with DoD 5220.22-M and the ITAR.

(1) Directorate of Defense Trade Controls (DDTC) forwards copies of agreements involving the release of classified articles (and related technical data) to DSS when related to U.S. contractors.

(2) DSS validates that the exporting U.S. contractor provides certification to the DoD transmittal authority that classified information does not exceed the technical or product limitations in the agreement and the U.S. exporting party (the U.S. contractor) will comply with the requirements of this manual and the ITAR.

(3) DSS validates that the exporter (U.S. contractor) provides certification to the transmittal authority (in the case of technical data exported pursuant to a technical data

exemption) that the technical data does not exceed the technical limitations of the authorized export in accordance with the ITAR.

(4) DDTC forwards licenses for the export of classified technical data or classified defense articles to DSS; and provides a copy to the applicant. DSS then takes actions as described in this section and returns the endorsed license to DDTC, upon completion of the export or the expiration of the license, whichever occurs first in accordance with the ITAR.

(5) DSS or another USG transmittal authority may require that a contractor produce relevant documents relating to exports of classified defense articles and technical data in accordance with the ITAR.

(6) DSS may take appropriate action to ensure compliance with this manual in the case of exports involving classified technical data or defense articles in accordance with the ITAR.

b. Bilateral security agreements and program-specific agreements require each signatory to safeguard classified information provided or generated under the agreement, and require that:

(1) The DSA in the signatory countries will be notified of contracts and other activities involving access to classified information by contractors for which they are responsible. The requirement to notify the DSA is based on the "government-to-government principle" governing international programs.

(2) Classified information will be transferred between government officials through government-to-government channels or through other channels agreed upon in writing by the DSAs of the responsible governments (referred to collectively in this manual as "government-to- government transfer").

(3) Classification guidance and security requirements clauses will be included in contracts involving access to classified information.

(3) (Added)(AF) The contracting officer will ensure security requirements and services for foreign military sales cases at foreign government locations are annotated on the DD Form 254 in block 13, Security Guidance. (T-0) The contracting officer will ensure the foreign government Cognizant Security Agency equivalent is identified in the DD Form 254 as the custodian of the releasable classified information and defense articles. (T-1)

(4) Access to classified information will be limited to persons who have appropriate security clearances and a need-to-know.

(5) The classified information will be provided substantially the same degree of protection required by the originator.

(5) (Added)(AF) The Implementing Designated Authority will conduct and/or coordinate site assessments and certifications of locations to verify security measures and

procedures prior to the delivery of the classified military information/defense articles and/or sensitive technology in Air Force foreign military sales cases with the Director, International Security programs, National Disclosure Policy Committee, Office of the Under Secretary of Defense for Policy. (T-0)

(6) The classified information will not be re-transferred to a third-party entity or used for any purpose other than that for which it was provided without the prior consent of the originator.

(7) Reports of loss or compromise or possible loss or compromise of classified information will be provided to the originating government.

c. United States Security Authority for NATO Affairs Instruction 1-07establishes and implements security standards to safeguard NATO classified information and also places restrictions on the use and retransfer of NATO classified information.

d. Providing special access program information to foreign nationals requires compliance with DoDD 5205.07.

12.3. EXCEPTIONS TO THE REQUIREMENTS OF THIS SECTION.

Deviations from the requirements in this section may have legal and foreign policy implications. Requests for exceptions to the procedures of this section must be documented, including alternative procedures, in accordance with Paragraph 3.3.a of this volume.

12.4. INTERNATIONAL PROGRAMS INVOLVING ACCESS TO U.S. CLASSIFIED INFORMATION BY FOREIGN GOVERNMENTS AND THEIR CONTRACTORS.

a. International programs may be initiated that require access to U.S. classified information by a foreign government or a foreign government contractor if:

(1) The classified information involved has been approved for export to the foreign government pursuant to the applicable U.S. export control laws, regulations, and foreign disclosure policies.

(2) The U.S. contractor has obtained the appropriate export authorization.

(3) The foreign government concerned has entered into a general security agreement or other security agreement with the USG under which the foreign government agrees to protect classified information disclosed to it or to contractors under its security jurisdiction.

b. If the international program is for FMS or another USG program (e.g., cooperative research, development, and acquisition program), the DoD FMS case implementing agency or the responsible program office will implement the security aspects of the program in coordination with the foreign government; further guidance regarding FMS programs is provided in DSCA Manual 5105.38. The DoD FMS case implementing agency or the USG

program office will consult and provide copies of required security documentation to assist DSS in maintaining security oversight of the U.S. contractor involved in the program.

(1) (Added)(AF) The Implementing Designated Authority will ensure holistic security elements and considerations are consistent across program offices and are included in the formally established security plan upon delivery of the Letter of Offer and Acceptance (LOA) to the partner nation. (T-1)

(2) (Added)(AF) The security plan establishes procedures and assigns responsibilities for implementation of security requirements required by the assigned case LOA for operations at the foreign government location. The plan should be developed by the program office prior to the LOA arrival and is intended to inform the purchasing country of the agreed upon general security requirements. The security plan will include instructions regarding the required protective measures associated with the classification of information and equipment; specifically, security procedures including the handling and transfer of classified materials, physical security parameters, visit procedures, and procedures for facilities that will be used to store and process classified information/defense articles and/or sensitive technology.

(3) (Added)(AF) In FMS cases, the program office will identify an individual responsible for assessing the fundamental requirements for secure storage and protection of classified information in overseas environments to reduce risks associated with the unauthorized disclosure of classified military information and critical technologies. (T-1)

c. If the program involves DCS, DSS will provide advice and assistance to the contractor that specifically notes that the contractor remains ultimately responsible for complying with U.S. export control laws and regulations. OUSD(P) Director, ISP will serve as the DSA, if a DCS requires approval of a program/project security instruction in the contract.

d. If a program involves exports by both a GCA and a U.S. cleared contractor (e.g., a hybrid program), DSS provides security oversight of contractor operations in accordance with the provisions of this manual to ensure compliance with established security requirements.

e. For classified contracts awarded to foreign contractors, the GCA will:

(1) Ensure that the contract contains security classification guidance in accordance with Section 6 of this volume and Volume 2 of DoDM 5200.01.

(2) Specify in the contract any limitations to be placed on the authority of the foreign contractor to award subcontracts.

(3) Ensure that the contract fixes responsibility for developing and obtaining approval for the necessary security plans, if there will be an anticipated need for the use of international carriers by the contractor for shipping classified material, a need for contractor employees to hand carry classified material, or a need for the contractor to use USG-approved secure communications.

(4) Request DSS obtain an FCLA on the foreign company from the DSA of the other government. This action verifies the FCL and storage capability and alerts the other government that a U.S. classified contract is to be awarded to one of the foreign government's contractors. Based on this notification, the other government must initiate the actions necessary to assume responsibility for safeguarding the U.S. classified information under the pertinent agreement.

(5) Provide a copy of the SCG and contract security clauses to DSS.

(6) For FMS and other USG programs involving a U.S. contractor, the FMS implementing agency or program office, as applicable, will, provide DSS with copies of required security documentation, in accordance with Paragraph 12.4.b of this volume and DSCA Manual 5105.38 to assist DSS in maintaining security oversight of the U.S. contractor involved in the program.

(7) Ensure that the security clauses, substantially as shown in Paragraphs 12.4.e.(7)(a) through 12.4.e.(7)(j) of this volume, are included, at a minimum, in all contracts involving classified information that are awarded to foreign contractors. In some cases, there may be a need to include provisions for other export controlled information, when the U.S. contractor is contractually obligated to provide specified safeguards for such information. GCAs must insert the bracketed contract specific information (e.g., applicable country or disposition of classified material) where noted, when using the security clauses in Paragraphs 12.4.e.(7)(a) through 12.4.e.(7)(j) of this volume in the contract. All classified information and material furnished or generated pursuant to this contract will be protected as follows:

(a) The recipient will not disclose or release the information or material to a third-country government, person, or company without prior USG approval.

(b) The recipient will afford the information and material a degree of protection equivalent to that afforded by the USG.

(c) The recipient will not use the information and material for other than the purpose for which it was furnished without prior written USG consent.

(d) Classified information and material furnished or generated pursuant to this contract will be transferred through government-to-government channels or through other channels specified in writing by the USG and [insert applicable country] and only to persons who have an appropriate security clearance and an official need for access to the information in order to perform on the contract.

(e) Classified information and material furnished under this contract will be marked by the recipient with its government's equivalent security classification markings.

(f) Classified information and material generated under this contract must be assigned a security classification as specified by the contract security classification specifications provided with this contract.

(g) All cases in which it is known or there is reason to believe that classified information or material furnished or generated pursuant to this contract has been lost or disclosed to unauthorized persons will be reported promptly and fully by the contractor to its government's national security authorities.

(h) Classified information and material furnished or generated pursuant to this contract will not be further provided to another contractor unless:

1. A potential contractor which is located in the United States or [insert applicable country] has been approved for access to classified information and material by the USG or [insert applicable country] security authorities; or

2. If located in a third country, prior written USG consent is obtained.

(i) Upon completion of the contract, all classified material furnished or generated pursuant to the contract will be [insert whether the material is to be returned or destroyed, or provide other instructions].

(j) The recipient will insert terms that substantially conform to the language of these security clauses (Paragraphs 12.4.e.(7)(a) through (j) of this volume) in all subcontracts under this contract that involve access to classified information or material furnished or generated under this contract.

f. When the international program is for DCS, DSS will:

(1) Initiate coordination with the designated DSA office of the recipient government to obtain the FCLA and ensure that the DSA has a copy of the SCG and contract security clauses.

(2) Provide advice and assistance, and approval for the USG, for the preparation and coordination of any transportation plan, hand carry plan, secure communications plan, visit arrangements, or other security documentation, ensuring that they are in compliance with the requirements of this manual.

(3) Monitor compliance by the U.S. contractor in accordance with the provisions of this manual.

(4) Notify the OUSD(I) CI&S and OUSD(P) Director, ISP when security issues arise that cannot be resolved between the U.S. contractor and the security authorities of the foreign government.

g. When the international program is for FMS or other USG program, DSS will:

(1) Request an FCLA on the foreign company from the designated DSA of the other government, when requested by the applicable FMS implementing agency or program office.

(2) Notify the FMS implementing agency or program office of the results of the FCLA, when received.

(3) Maintain security oversight of the U.S. contractor involved in the program in accordance with DoD 5220.22-M.

(4) Notify the FMS implementing agency or program office if the applicable transportation plan, hand carry plan, secure communications plan, visit arrangements, or other required security arrangements involving the U.S. contractor are not in compliance with this manual.

(5) Notify the OUSD(I) CI&S and OUSD(P) Director, ISP when security issues with security oversight of the U.S. contractor arise that cannot be resolved with the FMS implementing agency or program office.

12.5. INTERNATIONAL PROGRAMS INVOLVING ACCESS TO FGI BY U.S. CONTRACTORS.

a. This paragraph (12.5) applies to all international activities under which a U.S. contractor will have access to FGI. The laws, regulations, and agreements described in Paragraph 12.2 of this volume also apply to these activities and obligate USG compliance.

b. In addition to TS, SECRET, and CONFIDENTIAL, some foreign governments have a fourth level of classification, RESTRICTED, as well as another category of unclassified information that may be provided on the condition that it is treated in confidence. Foreign government markings are discussed further in Volume 2 of DoDM 5200.01 and for contractors in DoD 5220.22-M.

c. When notified by a U.S. contractor of any foreign government contract or other activity that will result in the U.S. contractor having access to FGI, DSS will:

(1) Request a copy of the applicable SCG and contract security clauses from the contractor as well as the approved export authorization (e.g., Department of State Form (DSP) 85, technical assistance agreement, or manufacturing license agreement), unless already provided by the DDTC. If an exemption of the ITAR applies, DSS may request the supporting documentation from the U.S. contractor.

(2) Oversee compliance by the U.S. contractor with contract security requirements, the provisions of this manual, and the security requirements in the ITAR.

(3) Act as the liaison between the U.S. contractor and the foreign government DSA regarding approved contract security matters.

(4) Provide advice and assistance on the preparation and coordination, and approval for the USG, of any transportation plan, hand carry plan, secure communications plan, visit arrangements, or other security documentation required, ensuring they are in accordance with

the provisions of this manual. OUSD(P) Director, ISP will serve as the DSA, if an international program requires approval of a program/project security instruction in the contract.

(5) Provide, when requested by the foreign government, the FCLA and the level of approved storage capability for U.S. contractors.

(6) Ensure, if foreign national visitors will be assigned to or visiting the contractor on approved intermittent visits, that the contractor has prepared a written TCP or other written technology control procedures that address the requirements and elements of information equivalent to a TCP. DSS will post a TCP format that may be tailored for a specific case on its website. When a document other than a TCP is used, the section that deals with TCP issues should be in a separate section, such as an section, so it can be removed to facilitate compliance with the ITAR, as well as orientation of foreign national employees and visitors.

(7) Contact the DSA of the foreign government concerned if DSS determines that classified information has not been properly transferred. DSS will also contact the DSA of the foreign government concerned if DSS learns of a classified contract or other initiative involving FGI for which the U.S. contractor or the contracting foreign government did not provide notification. In such cases, DSS will arrange for appropriate instructions to be provided by the DSA of the foreign government to DSS and to the U.S. contractor. If unable to resolve the issue, DSS will refer the matter to the OUSD(I) CI&S and to the OUSD(P) Director, ISP for coordination and resolution.

12.6. TRANSFERS OF CLASSIFIED INFORMATION AND MATERIAL TO FOREIGN GOVERNMENTS.

After a USG decision is made to authorize the export of classified information or material to a foreign government, the transfer may occur as oral or visual disclosures between individuals during international visits, or the information may be transferred in material or electronic form. Export requirements for DCS programs are stated in the ITAR and in DSCA Manual 5105.38 for FMS programs. Detailed security requirements pertaining to international transfers are contained in Volume 3 of DoDM 5200.01 and DoD 4500.9-R. Section 7 of this volume includes information with regard to transfers of defense articles to the United Kingdom (U.K.) and Australia without a license or other written authorization for implementation. Policy for transfers of COMSEC information and material to foreign governments are contained in CNSSP 8, CNSSI) 4005, and applicable Component specific policy (e.g., NSA/CSS Service Policy Manual 3-16).

a. Classified information and material will be transferred to a foreign government between government officials and through official government-to-government channels, or through government-to-government transfers. A detailed, written plan must be prepared, providing for government oversight and control of transfers from the point of origin to the ultimate destination, when other than official government-to-government channels are used (see Paragraph 12.6.c of this volume for the specific procedures that must be included in the detailed, written plan).

a. (Added)(AF) The Air Force Security Assistance and Cooperation Directorate (AFSAC), assigned as the Air Force Implementing Agency and International Logistics

Control Organization, ensures U.S. government accountability and control by incorporating written instructions for all transfers of classified material. The transportation plan will describe step-by-step arrangements for the secure shipment of the classified material from the point of origin to the final destination. This plan must be approved by the AFSAC Transportation Office prior to transferring classified material to the partner nation. (T-1)

b. TS information and material will be transferred between government officials only through official government-to-government channels using USG approved information technology (IT) or communications systems, the U.S. Transportation Command's Defense Courier Division (TCJ3-C)), authorized USG agency courier services, the DoS Courier Service, or a properly cleared and briefed USG agency employee designated as a courier.

c. Instructions relating to transfers of SECRET and CONFIDENTIAL information or material by contractors and DSS oversight of such transfers are provided in Paragraphs 12.8 through 12.14 of this volume. Transfers of SECRET and CONFIDENTIAL information or material that are not transferred by government officials through official government-to-government channels may be:

(1) Transferred as freight, using a transportation plan.

(2) Hand carried, using a hand carry plan with appropriately cleared U.S. contractor employees authorized to hand carry classified material of a size and weight over which the employee can maintain personal control.

(2) (Added)(AF) In support of FMS cases, the AFSAC Transportation Office and the program office official responsible for security requirements in accordance with Paragraph 12.4.b.(3) of this volume must approve the need to hand carry SECRET and CONFIDENTIAL information or material to ensure the appropriate transfer arrangements are made and to establish responsibilities for the transfer arrangements prior to the execution of the agreement or contract. (T-1)

(3) Transmitted by contractor employees using USG-approved IT or communications systems, under a secure communications plan, all to be approved by both sending and receiving governments.

d. GCAs will ensure that contracts with foreign governments or foreign contractors assign responsibilities and contain procedures for preparing and approving plans for the international transfer or transmission of classified information and material. The procedures will include instructions and the assignment of responsibility for shipment and subsequent receipt in the United States of classified articles that are to be returned to the United States for repair, overhaul, or maintenance (ROM). DSS will ensure that the appropriate DSS office has the original copy of the DSP-85, upon notification by a U.S. contractor that is to receive the ROM shipment.

e. Transfers of FGI classified RESTRICTED or unclassified, provided in confidence, will

be made in accordance with Volume 3 of DoDM 5200.01.

12.7. TRANSFERS OF DEFENSE ARTICLES TO THE U.K. AND AUSTRALIA WITHOUT A LICENSE OR OTHER WRITTEN AUTHORIZATION.

a. The "Treaty Between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland Concerning Defense Trade Cooperation" and the "Treaty Between the Government of the United States of America and the Government of Australia Concerning Defense Trade Cooperation" provide a comprehensive framework for exports and transfers to the U.K. or Australia of classified and unclassified defense articles without a license or other written authorization. Implementation of certain aspects of "Treaty Between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland Concerning Defense Trade Cooperation" occurred through amendment of the ITAR, Volume 3 of DoDM 5200.01, and DSCA Manual 5105.38. Implementation of certain aspects of the "Treaty Between the Government of the United States of America and the Government of Australia Concerning Defense Trade Cooperation" will occur upon amendment of the ITAR, Volume 3 of DoDM 5200.01, and DSCA Manual 5105.38.

b. DSS will verify that contractors comply with the provisions of DoD 5220.22-M and the ITAR as amended for transfers of classified defense articles consistent with the "Treaty Between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland Concerning Defense Trade Cooperation" and the "Treaty Between the Government of the United States of America and the Government of Australia Concerning Defense Trade Cooperation".

c. GCAs will implement the applicable provisions of the "Treaty Between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland Concerning Defense Trade Cooperation" and the "Treaty Between the Government of the United States of America and the Government of Australia Concerning Defense Trade Cooperation" when applicable guidance is amended or updated (i.e., the ITAR, Volume 3 of DoDM 5200.01 and DSCA Manual 5105.38.

12.8. RESPONSIBILITIES OF A U.S. DESIGNATED GOVERNMENT REPRESENTATIVE (DGR).

a. The basic responsibilities of the U.S. DGR are established by the ITAR and Volume 3 of DoDM 5200.01. The ITAR requires that a DoD or other USG transmittal authority oversee the transfer of classified defense articles and technical data. Volume 3 of DoDM 5200.01 specifies that classified information will be transferred between government officials through official government-to-government channels, or government-to-government transfer. Agreements with other governments specify that classified information will be transferred through official government-to-government channels or other channels that are agreed to in writing between the governments. The DGR requirement establishes USG oversight and ensures that proper security safeguards are in place and enforced when other than official government-to-government

channels are used for transfers of classified defense articles and technical data. DSS has been assigned this responsibility by DoDD 5105.42 and the ITAR.

b. The DGR functions involve:

(1) Transfers of classified material as freight provided in Paragraph 12.12 of this volume.

(2) Hand carriage of classified material provided in Paragraph 12.14 of this volume:

(3) Transfers of classified information by secure communications transmissions provided in Paragraph 12.15 of this volume.

c. When a DSS representative or another USG official is not readily available to perform the DGR functions in a timely manner as described in Paragraphs 12.12, 12.14, or 12.15 of this volume, DSS may authorize the contractor to oversee the actual transfer of the classified information and material, if:

(1) The contractor's FSO and empowered official provide DSS, in advance, a joint, written certification that DSS-approved requirements for such transfers, in accordance with DoD 5220.22-M, have been satisfied.

(2) DSS reviews all of the other required documentation as described in Paragraphs 12.12, 12.14, or 12.15 of this volume and either approves the transfer or transmission procedures described in the joint written certification; approve them subject to further action on the part of the GCA or cleared contractor, as applicable; or disapproves the security procedures.

(3) DSS will follow-up as soon as possible and verify the contractor's compliance with the requirements of DoD 5220.22-M when the procedures in Paragraph 12.8.c of this volume are used.

(4) DSS will ensure that delegated DGRs are provided adequate guidance to allow them to perform the DGR responsibilities.

12.9. TRANSPORTATION PLANS. A transportation plan will be developed for the transfer of CONFIDENTIAL and SECRET material as freight. While the transfer of title and custody to classified material may occur at a USG depot, contractor, or FF facility, security responsibility remains with the USG until the recipient government's DGR or DGR-designee in accordance with Paragraph 12.12 of this volume signs for the material.

12.9. (Added)(AF) Transfers of classified information and material to foreign governments will be made in accordance with the Foreign Trade Regulations and the International Traffic in Arms Regulations with regard to export reporting to U.S. Customs and Border Protection.

a. A transportation plan is required for all transfers of SECRET and CONFIDENTIAL

freight across international borders, regardless of the sale mechanism being used, i.e., DCS or FMS.

a. (Added)(AF) A transportation plan for FMS cases involving the transfer of classified information to a foreign partner is required even when the transfer occurs within the United States.

(1) A transportation plan must provide detailed guidance for the initial transfer and for any return shipments for follow-on support, such as maintenance, repair, and upgrades. Volume 3 of DoDM 5200.01 provides the required elements of a transportation plan.

(2) The approved transportation plan template for FMS is in DSCA Manual 5105.38; this plan also may be used for DCS. DSS will maintain the same transportation plan template on its website (www.dss.mil) to ensure standardization of transportation plans.

b. DSS will approve the transportation plan for DCS programs and forward it to the recipient government's DSA, or their designated government official, for coordination and approval. The transportation plan for DCS will be prepared by the U.S. contractor and the purchasing government's representative or the purchasing government's designated FF in accordance with DoD 5220.22-M.

c. The DoD FMS case implementing agency, in coordination with its supporting security and transportation officials, and the purchasing government, will develop and approve a transportation plan for FMS programs. The DoD FMS case implementing agency will consult with the GCA supporting transportation officials to determine if USG-owned or registered transportation is available, prior to any commitment to use other than government transportation.

(1) Security and transportation officials of the DoD FMS case implementing agency will evaluate the adequacy of the transportation plan, and are authorized by Volume 3 of DoDM 5200.01 and DSCA Manual 5105.38 to delay any transfer until the plan meets the standards prescribed by this manual.

(2) The DoD FMS case implementing agency will provide a copy of the approved transportation plan to:

(a) The U.S. contractor that is involved in the transfer.

(b) An FF, if one is to be used in processing the shipment.

(c) DSS, for its information in exercising oversight of the U.S. contractor.

12.10. ESCORTS. Pursuant to DSCA Manual 5105.38, SECRET or CONFIDENTIAL material transferred internationally to foreign governments will be accompanied by escorts who are provided by the DoD FMS case implementing agency or the contractor for DCS, as applicable, and cleared to the level of the material to be shipped. The only exceptions to the

requirement are:

a. The material is shipped by U.S. military carrier and the crew assumes control of the material.

b. The recipient government DGR has signed for the consignment, a recipient government military carrier or carrier owned by or registered to the recipient government is used, and the recipient government provides the cleared escort.

c. In exceptional circumstances, with the written approval of the sending and receiving government DSAs, and provided:

(1) The material is stored in the hold of an aircraft of a U.S. owned or registered air carrier or an air carrier owned by or under the registry of the recipient government.

(2) The shipment is placed in a compartment that is not accessible to any unauthorized person or in a specialized shipping container approved for this purpose in accordance with DSCA Manual 5105.38.

(3) The air carrier agrees in writing to permit a cleared DoD or cleared U.S. contractor employee, specifically designated by name, to observe placement of the classified consignment into the aircraft.

(4) The flight is direct, between two designated points, with no intermediate stops.

(5) The air carrier agrees in writing that a designated officer on the aircraft will assume responsibility for the classified consignment while en route to the destination.

(6) Written emergency instructions are provided to the air carrier.

(7) Arrangements are made for recipient foreign government DGR or other DGR-designated official, designated by name, in writing, to be present at the unloading of the consignment and immediately assume security control for the recipient government.

(8) The foregoing requirements are documented in the transportation plan.

(9) The exceptional circumstances are documented in the request for exception.

12.11. FFS. A GCA, a U.S. contractor, or a foreign government may contract with a cleared FF to facilitate transportation arrangements for material classified no higher than SECRET. Section 4 of this volume includes the FCL requirements for the three types of FFs. Criteria for use of a cleared FF are:

a. An FF can only be used with the concurrence of both the sending and receiving governments and must:

(1) Be designated in writing.

(2) Possess the requisite level of FCL if it is to have possession of classified material at any time.

(3) Be registered with the DDTC.

b. Volume 6 of the Defense Logistics Manual 4000.25 may be consulted to identify approved FFs. However, the FF's FCL should be verified by DSS.

c. An FF may be used by multiple countries as long as the DSA of the government of all countries using that FF, DSCA, and OUSD(P) Director, ISP approve such use.

d. A U.S. FF will not be the point of ultimate destination for a classified consignment and will not be designated by a foreign government as its DGR, because a cleared FF is under U.S. (not foreign government) security control.

e. FFs are not authorized pursuant to Volume 3 of DoDM 5200.01 to handle certain sensitive arms, ammunition, and explosives (AA&E).

12.12. SHIPMENTS USING A TRANSPORTATION PLAN. For contractors using a transportation plan and transferring classified material by shipping it as freight, DSS will:

a. Advise U.S. contractors on the necessary transfer arrangements, to include ensuring that the required export authorizations have been obtained, and that the transfer arrangements comply with USG and NATO standards and applicable security agreements.

b. Confirm the identity of the recipient government's designated DGR for the transfer and an alternate (e.g., including name, position, location, and contact information).

c. Assign a DSS employee to perform the DGR functions or authorize a contractor as provided in Paragraph 12.8.c of this volume. Even if certain DGR-related functions are assumed by a representative of another USG agency, DSS will maintain oversight responsibility for the overall government-to-government transfer process for classified data and material and will verify compliance by the U.S. contractor.

d. Ensure that the DGR, when there is a transfer of classified material as freight:

(1) Obtains the export authorization from the U.S. contractor.

(2) Verifies that the contractor has the appropriate documentation (e.g., DSP-85, technical assistance agreement, or manufacturing license agreement) in those instances where:

(a) The DDTC has not already provided the export authorization to the DSS, in

accordance with the ITAR or;

(b) The DGR obtains supporting documentation when the ITAR, exemption is used.

(3) Checks the export authorization for any special provisos related to security and verifies that they are met.

(4) Verifies that the transportation plan:

(a) Meets the requirements specified in this section.

(b) Contains the elements of information in the example at www.dss.mil or in DSCA Manual 5105.38.

(c) Reflects the same destination country, consignee, and end-user as specified in the export authorization.

(d) Has been approved by both the USG and the recipient foreign government security authorities.

(5) Confirms that there will be a continuous chain of receipts.

(6) Verifies by on-site inspection or obtains certification from the U.S. contractor's empowered official that:

(a) The contents of the consignment have been visually observed.

(b) The material is properly packaged, marked, wrapped, sealed, and addressed.

(c) The classified defense articles or technical data to be exported are as described in the export authorization.

(7) Notifies DSS if the requirements of Paragraphs 12.12.d.(1) through 12.12.d.(5) of this volume are not met, providing recommended actions to be taken. DSS will then notify the FMS case implementing agency (for FMS), the program or project manager (for other DoD programs), or contractor senior security official (for DCS) to seek resolution of the matter.

e. Coordinate transfer arrangements with the recipient foreign government DSA to ensure there is government oversight and accountability from the point of origin to the ultimate destination and the recipient foreign government concurs in the arrangements. Once DSS (for the USG) and the foreign government have approved the arrangements, DSS will confirm with the U.S. contractor for DCS that coordination has been made with U.S. security, customs, and immigration organizations at the port of embarkation to facilitate the secure and timely movement of the classified material involved. DSS will confirm that the recipient government has completed similar coordination with the equivalent authorities in the recipient country.

f. Immediately notify the DSA of the other country and the responsible U.S. contractor, if DSS determines that the necessary arrangements have not been completed for a DCS program and provide advice on completing the arrangements. If prescribed arrangements are not completed satisfactorily in a reasonable period of time (e.g., prior to scheduled shipment and DSS is unable to obtain agreement by the foreign government that changes to the schedule should be made), notify the OUSD(I) CI&S and the OUSD(P) Director, ISP who will consult to assist DSS in resolving the matter with the U.S. contractor and the recipient government.

g. Authorize the release of the classified material, provided there is an approved export authorization and the transportation plan and related arrangements meet prescribed standards as described in the template jointly approved by the OUSD(I) CI&S and OUSD(P) Director, ISP at www.dss.mil.

h. Notify the FMS case implementing agency, if DSS has concerns with an FMS transportation plan to be used by a U.S. contractor or other aspects of the transfer, providing the details of the concerns and the possible consequences if they are not resolved.

(1) If the GCA or FMS case implementing agency do not satisfactorily resolve the concerns, provide notice of the issues to the DSCA, with an information copy to the OUSD(I) CI&S and OUSD(P) Director, ISP.

(2) DSCA will take action to resolve the matter in coordination with OUSD(I) CI&S and OUSD(P) Director, ISP, if so notified of the concerns by DSS.

i. Return the endorsed export authorization to DDTC for DCS, when:

(1) The total value authorized has been shipped, plus or minus 10 percent.

(2) The contractor states there will be no further shipments.

(3) The date of license expiration is reached.

(4) Requested by DDTC.

12.13. USE OF INTERNATIONAL CARRIERS. Only international carriers that are owned by or registered with the USG, or are owned by or registered with a recipient government, are otherwise authorized by the DSAs of the sending and receiving governments to be used to transfer classified material. Escort requirements specified in Paragraph 12.10 of this volume apply.

12.14. INTERNATIONAL HAND CARRYING OF CLASSIFIED MATERIAL.

a. GCA personnel designated to hand carry classified material will comply with the provisions of Volume 3 of DoDM 5200.01.

b. DSS may authorize appropriately cleared U.S. contractor employees to hand carry classified material for a specific USG-approved program, project, or contract, cooperative arms program, or for a DCS, when there is a demonstrated need to do so, provided:

(1) The contractor obtains approval from the applicable GCA for the specific USG program, project, or contract or from the foreign government contracting activity for a DCS program.

(2) DSS coordinates and obtains concurrence on the hand carry plan with the authorized representative of the recipient foreign government's DSA to ensure the plan provides for the safe and secure transfer of classified information from point of origin to final destination.

(3) The highest level of classified material to be transferred in this manner will not exceed the SECRET level and must be of such size, weight, and configuration that hand carriers can retain it in their personal possession at all times until it is delivered to the foreign government's DGR or other designated person.

(4) The contractor has made arrangements for overnight storage at a USG-controlled location, if overnight stops are necessary.

(5) U.S. contractor employees designated to hand carry classified material have a courier authorization and ensure that all documentation required by carrier security authorities and port security, immigration, and customs officials is in place.

c. DSS will exercise oversight of a U.S. contractor's compliance with an approved hand carry plan for DCS and FMS programs.

d. When classified material is being hand carried internationally by contractor employees, DSS will:

(1) Verify that the U.S. contractor has procedures in place requiring the U.S. contractor's empowered official to certify in writing for each such hand carriage that the classified material and or associated technical data being shipped is within the scope of the approved export authorization.

(2) Verify that the hand carry plan meets the standards specified in this manual; the courier has been briefed on responsibilities and actions to take in emergency situations; and the courier has the prescribed courier orders, required travel documentation, and an authentic courier certificate.

(3) Review and approve the proposed security procedures, including providing assistance in coordinating with other USG organizations, such as security, customs, and immigration, as appropriate.

(4) Verify that the DSA of the country of destination approves the in-country security arrangements; confirm the intended recipient is authorized to receive, handle, and store the

classified material; and identify the foreign government DGR.

(5) Ensure that the receipt for the material is returned with the hand-carrier, and determine whether any incident occurred that may have placed the classified material in jeopardy; initiate an inquiry if deemed necessary.

e. When classified material must be hand carried by representatives of a foreign government to a U.S. contractor location that has the appropriate FCL and safeguarding capability, DSS will:

(1) Coordinate the hand carry plan with the authorized representative of the recipient foreign government's DSA to ensure the plan provides for the safe and secure transfer of classified information from point of origin to final destination.

(2) Verify the FCL and storage capability of the receiving U.S. contractor.

(3) Verify with the U.S. contractor that coordination has occurred with appropriate U.S. port security authorities and with U.S. immigration and customs officials.

(4) Ensure that a DSS employee or a designated person identified in the hand carry plan will be available to receive the material and complete the government-to-government transfer.

f. When there is a hand carriage of classified material, the DGR, in addition to the functions described in Paragraphs 12.12.d.(1) and 12.12.d.(4) of this volume, will:

(1) Verify that the hand carry plan:

(a) Meets the requirements specified in Paragraph 12.14 of this volume.

(b) Contains the elements of information specified in the example on www.dss.mil.

(c) Reflects the same destination country, consignee, and end-user as specified on the export authorization.

(d) Has been approved by both the USG and recipient foreign government security authorities.

(2) Obtain a written certification from the U.S. contractor's empowered official that the classified defense articles or technical data being hand carried are as described in the export authorization.

(3) Notify DSS if the requirements of Paragraph 12.14.f.(1) and 12.14.f.(2) of this volume are not met, providing recommended actions to be taken. DSS will notify the FMS case implementing agency for FMS, or the contractor senior security official headquarters, for DCS, to seek resolution of the matter.

12.15. SECURE COMMUNICATIONS.

a. USG approved IT and communications equipment and procedures are required for the protection of U.S. classified information and FGI transmitted via voice, facsimile, or data between a foreign government or a foreign contractor and a U.S. contractor. The U.S. contractor must have an FCL, the appropriate export authorizations and maintain records in accordance with the Component or GCA record-keeping manual, to ensure adequate safeguarding capability, and a USG COMSEC account.

b. All foreign COMSEC equipment and keying material authorized for use must be protected under the U.S. contractor's COMSEC account and NSA/CSS must approve the use of the equipment. NSA/CSS will approve the access, use, and release of NSA/CSS-endorsed COMSEC equipment for international programs. Security authorities of both governments will approve the security arrangements used to transfer the information and equipment between governments. Prior to the exchange of classified information, cryptographic information, or the COMSEC equipment, the government security and COMSEC authorities must approve a secure communications plan that specifies the required level of protection and security assurances.

c. For USG programs, projects, or contracts, the GCA will notify NSA/CSS in writing of the requirement and provide a plan containing the information required by this paragraph. If NSA/CSS approves a plan for a contractor, the GCA will provide a copy of the NSA/CSS approved plan to DSS. DSS will post a template for a secure communications plan, coordinated with NSA/CSS, on www.dss.mil. The approved template for secure communications plans will include:

(1) The purpose the request and the contract number, or other program or project identification.

(2) The identity of the entities involved.

(3) The description and classification of the information involved.

(4) A description of the transmission requirement, to include the medium (voice, data, facsimile) and speeds.

(5) A description of the secure communication equipment to be used.

(6) Procedures for authorizing individual exports and identify the associated Component or GCA records disposition for export records.

(7) A statement on the funding required for procurement of the necessary equipment and source of funding.

(8) Procedures for auditing transmissions, at a minimum, to ensure that the intended

recipient received the information in accordance with DoD 5220.22-M.

d. For the use of secure communications for transmission with a foreign government by a U.S. contractor, DSS will:

(1) Provide advice on the preparation of the contractor's secure communication plan.

(2) Evaluate and approve the contractor's IT system and communications equipment and procedures to be used for secure communications.

(3) Forward the contractor's proposed secure communication plan to NSA/CSS and, after NSA/CSS approval, to the foreign government's security authority for final approval.

(4) Review a contractor's compliance with secure communications plans for USG programs, projects, and contracts and direct commercial sales as part of the periodic security review.

e. Transfers of COMSEC or controlled cryptographic items will be accomplished in accordance with CNSSI 4001, CNSSI 4005, and any Component specific guidance (e.g.,National Security Agency/Central Security Service (NSA/CSS) Policy Manual 3-16).

f. When there are transfers or transmissions of classified information by secure communications, the DGR, in addition to the functions in Paragraphs 12.12.d.(1) and 12.12.d.(2) of this volume, will:

(1) Verify that the secure communications plan meets the requirements specified in Paragraphs 12.14.f.(1)(a) through 12.14.f.(1)(d) of this volume.

(2) Verify that the U.S. contractor complies with DoD 5220.22-M.

(3) Obtain a written certification from the contractor's empowered official that the contractor has procedures in place to ensure that information to be transmitted is as specified in the applicable export authorization.

(4) Notify DSS if the requirements of this section are not met, providing recommended actions to be taken. DSS will notify the FMS case implementing agency for FMS, or the contractor senior security official headquarters, for DCS, to seek resolution of the matter.

12.16. INTERNATIONAL VISITS, ASSIGNMENTS OF FOREIGN NATIONALS, AND CONTROL OF FOREIGN NATIONAL EMPLOYEES.

a. Visits by Foreign Nationals to U.S. Contractors and Control of Foreign National Employees. DoDD 5230.20 establishes the requirements and procedures to control visits and assignments of foreign nationals (hereinafter referred to as "foreign representative") who represent or are sponsored by a foreign government to U.S. contractor facilities under the

international visits program. The foreign visit system (FVS) is the automated system used for processing requests for visits (RFV) by foreign representatives to DoD facilities and U.S. contractors. RFVs for such persons must include a security assurance if the visitor is to have access to classified information. Only a foreign representative for whom a security assurance has been provided will have access to classified information, even though an export or disclosure authorization may have been obtained from DDTC or a DoD disclosure authority. The process for RFVs for U.S. contractors to visit foreign government organizations and foreign companies is in DoD 5220.22-M.

(1) DSS will, as the CSO:

(a) Verify that the U.S. contractor:

1. Designates an employee to act as a point of contact for all foreign representatives assigned to a U.S. contractor or visiting a U.S. contractor under a RFV in accordance with DoD 5220.22-M.

2. Has a written TCP or equivalent procedures that contains all of the elements of a TCP as required by DoD 5220.22-M.

3. Has an export authorization to disclose export controlled technical data to foreign representative visitors as required by DoD 5220.22-M, even though the disclosure may occur on a GCA installation or in the presence of GCA officials.

(b) Provide the U.S. contractor with a TCP template approved by OUSD(P) Director, ISP and OUSD(I) CI&S, and guidance necessary for the contractor to tailor the written TCP to meet specific circumstances.

(c) Approve the U.S. contractor developed TCP and periodically evaluate the effectiveness of the TCP as part of the ongoing oversight of the U.S. contractor's security program, which will include interviews with contractor employees who work with the foreign nationals, as well as contractor officials who oversee policy implementation.

(d) Meet with contractor employees designated as points of contact for foreign national visitors and employees and to verify training, and assign employee responsibilities based on DoD governing policies.

(e) Publish a jointly approved OUSD(I) CI&S and OUSD(P) Director, ISP format and guidance on the DSS website (www.dss.mil) to enable the contractor to prepare the request for visit authorization correctly.

(2) DSS may, in its role as the CSO:

(a) Grant an exception for a specific TCP, if the contractor has in place other written procedures which readily identify the requirements and elements of information equivalent to a TCP.

(b) Authorize the U.S. contractor to furnish a foreign national visitor with a security container at the contractor facility for the temporary storage of classified material consistent with the purpose of the visit or assignment. If authorized by DSS, the following provisions, at a minimum, apply:

1. The need for the container will be documented in the pertinent RFV or in a separate written request to the contractor by the visitor's government.

2. The request will acknowledge that the work area and the container will be under the security control of the U.S. contractor.

3. Receipt of classified material furnished to the visitor by the visitor's government will be through official government-to-government channels. The storage container, work area, and procedures used by the foreign national visitor will be subject to periodic review by DSS.

b. Disclosures of Unclassified Technical Data by U.S. Contractors. DoD 5220.22-M provides the requirements and procedures for U.S. contractors regarding RFVs by foreign representatives related to disclosures of unclassified technical data related to:

(1) DoD classified programs.

(2) A contract requirement even though the foreign representative does not represent or is not sponsored by a foreign government.

(3) A commercial program for which the contractor has an export authorization.

(4) Information to be divulged is in the public domain.

c. Receipt of RFVs by U.S. DoD Defense Visits Offices (DVOs). The responsible U.S. DoD DVOs will receive RFVs by foreign representatives through the sponsoring government's embassy in Washington, DC, using the FVS. RFV and DVO responses are the vehicles for recording the disclosure authorization decision and obtain the security assurance on the foreign representative visitors.

d. Types of Visit Authorizations. There are three types of visit authorizations.

(1) One-Time Visit Authorization. This type will be used to document a single, short-term visit; there is no known requirement for subsequent visits; and the conditions for a recurring visit authorization or extended visit authorization do not apply.

(2) Recurring Visit Authorization. This type will be used to document intermittent, recurring visits. It is to be used in support of government approved and documented programs, agreements, export authorizations, and contracts when the foreign disclosure decision or export authorization has been approved.

(3) Extended Visit Authorization. This type will be used to certify national representatives and foreign liaison officers who are stationed at their embassies and are authorized to conduct business with the DoD GCAs, operating from their embassies. It also will be used to document the assignment of each foreign representative to a DoD Component or a U.S. contractor. A GCA assignment of a foreign representative visitor to a U.S. contractor on an extended visit authorization will be coordinated in advance with the contractor and with DSS. Only an FMS liaison officer or a foreign representative assigned to a cooperative arms program may be assigned to U.S. contractor. The terms of the assignment will be documented in the contract between the GCA and the contractor.

e. Responses to RFVs. DoD officials will not approve visits to a U.S. contractor location by a foreign representative for a DCS program; the contractor must obtain an export authorization. The DoD DVOs will provide one of the four responses to an RFV:

(1) Approved. If access to requested information supports an actual or planned government program, and disclosure of the information or technical data is authorized, the DVO will approve the RFV and provide disclosure guidance.

(2) Non-Sponsored. If a proposed visit is not in support of a government program (rather, it supports a commercial program), the DVO will not approve the RFV because assisting a contractor for a commercial effort would be in violation of the ITAR. However, if the responsible DoD GCA would not object to the visit, provided the proper export authorization is in place, the DVO will notify the requester and applicable U.S. contractor that arrangements for the visit may be made directly between the requester and the contractor, provided the U.S. contractor has or obtains an export authorization for any export-controlled technical data that may be disclosed. This action is commonly referred to as a "non- sponsored" visit. The DVO will forward the security assurance that has been provided by the foreign government to the U.S. contractor. If the security assurance has not been provided, the DVO's response will notify the requesting government or organization and the U.S. contractor that a security assurance will be required before classified information may be divulged during any directly arranged visit.

(3) Denied. The DVO will deny the RFV, if it is determined that the information associated with the proposed visit cannot be authorized for disclosure. The DVO will notify the requester and the applicable U.S. contractor of the decision. The denial of the request does not prevent the contractor from accepting the visit provided the contractor has an export authorization for other export-controlled information that may be disclosed.

(4) Returned Without Action. If the purpose of the visit is not adequately explained or justified, the information or technical data to be disclosed is not described in sufficient detail, the locations to be visited cannot be readily discerned, the security assurance is not provided, or the request is not received in ample time to process, the RFV will be denied or returned without action, with the specific reasons for return described in the response.

f. Exemption to the Export License. In accordance with the ITAR, a request for an

official visit to a U.S. contractor that is approved by a DVO may serve as the basis for a contractor to claim an exemption to the export license requirements of the ITAR but only when the visit is in support of a government program and the technical data to be disclosed is fully described in the RFV or DoD response. The RFV also must identify the U.S. contractor, the end use for the information, and end-user.

g. Data Retention Requirements for an Approved RFV. The ITAR provides the data retention requirements when technical data is disclosed to foreign representatives during a visit.

h. U.S. Contractor Employee Visits to Foreign Governments and Foreign Contractor Facilities. DoD 5220.22-M provides the requirements to ensure U.S. contractor employees have the necessary export authorizations, meet all security requirements, and follow the prescribed format and procedures for international visits. DSS will, as the CSO:

(1) Verify the PCLs of the contractor employees making the overseas visit.

(2) Assure that need-to-know is established by a license, agreement, or FMS case.

(3) Add the U.S. security assurance for the contractor employee(s).

(4) Forward RFVs to the in-country USG office designated in the Department of Defense Foreign Clearance Guide to coordinate the visits.

(a) DSS may obtain information from the contractor to complete the RFV, or return the request to the contractor's security office to be corrected, if the contractor does not provide the prescribed information.

(b) DSS will not knowingly forward to the designated USG office in-country RFVs that fail to comply with established requirements.

12.17. U.S. CONTRACTOR OPERATIONS OUTSIDE OF THE UNITED STATES, ITS TERRITORIES, OR THE DISTRICT OF COLUMBIA.

When U.S. contractor employees are assigned in foreign countries, they may have access to classified information in accordance with DoD 5220.22-M. DSS will advise U.S. contractors on security requirements for contractor employees assigned or visiting outside the United States. Section 3 of this volume provides the Commander's roles and responsibilities for U.S. (cleared or uncleared) company visitors or U.S. contractor facilities on USG installations. In foreign countries, DSS will only exercise security cognizance for contractor locations with FCLs on USG-controlled installations, unless the Commander retains security cognizance of the FCL in accordance with Section 3 of this volume. Section 4 of this volume provides criteria to sponsor an FCL for a U.S. contractor, including those located on a USG or USG-controlled installation in a foreign country.

a. Storage of U.S. Classified Information and Material in a Foreign Country.

(1) The storage of classified material by U.S. contractor employees at any location in a foreign country other than a USG-controlled location, as described in Volume 3 of DoDM

5200.01, is prohibited unless an exception to the requirement is approved in accordance with Section 3 of this volume. GCAs or FMS case implementing agencies will consult with U.S. contractors prior to signing contracts involving U.S. company operations in a foreign country, to determine if there will be a need to store classified information in the foreign country in compliance with Volume 3 of DoDM 5200.01.

(1) (Added)(AF) The acquisition program office will assess the secure storage needs and ensure requirements are defined in the Request for Proposal, Statement of Objectives, or Statement of Work prior to the contract award. (T-1) The program office will take into consideration the type of classified material involved to ensure specific security requirements are applied. (T-1)

(2) Procedures for storage of classified information by a U.S. contractor location with an FCL on a USG-controlled location in a foreign country, are located in Paragraph 12.17.c of this volume.

(3) The Commander or a GCA on a USG-controlled installation in a foreign country may furnish a security container for a U.S. contractor visitor to temporarily store classified information on the installation. In these instances:

(a) The contract or program agreement must require storage of U.S. classified information at the installation.

(b) The decision to permit the contractor employee visitors to temporarily store the classified information must be approved in writing by the senior security official of the GCA or the Commander, in coordination with the senior security official at the installation.

(c) The contractor employee visitor will be subject to the security procedures of the USG host organization, or if applicable, of the Commander.

(d) The USG security officer at the USG-controlled installation will report any security violation of the security arrangements to DSS to include in its oversight of the U.S. contractor's HOF in the United States. DSS will also make compliance with the requirements a matter of special interest during its oversight of the U.S. contractor's HOF in the United States.

(4) The Commander or the responsible GCA at the USG-controlled installation may permit U.S. contractor employee visitors to temporarily remove classified information from a USG-controlled location, when necessary for contract performance for a USG organization, or pursuant to an approved export authorization, if the information is in support of a foreign government or NATO requirement. When removal is permitted, the Commander or GCA will:

(a) Verify that the contractor employee visitor has an export authorization or other written USG approval to have the material.

(b) Verify the need for the material to be removed from the location.

(c) Brief the contractor personnel on handling procedures.

(d) Obtain a signed receipt for the classified material from the contractor employee.

(e) Verify that arrangements have also been made for the return and storage of the classified material during non-duty hours.

b. Exception Requests for Storage of Classified Information and Material in a Foreign Country. If a GCA determines that retention and storage of U.S. classified information by a U.S. contractor is necessary to perform on a contract or agreement in a foreign country, and the location where work is to be performed is not on a USG-controlled installation, the responsible GCA may request an exception, in accordance with the May 20, 2016 USD(I) Memorandum, "Clarification of Overseas Protection Requirements for Classified Information" and Section 3 of this volume.

c. Safeguarding Approval for an FCL on a USG-Controlled Installation in a Foreign Country.

(1) The CSO may approve safeguarding capability for a U.S. contractor location with an FCL established as a tenant on a USG-controlled installation in a foreign country in accordance with the pertinent provisions of this manual. The arrangement must be endorsed in writing by the Commander or the responsible GCA on the USG-controlled installation who is sponsoring the FCL.

(1) (Added)(AF) Refer to Paragraph 3.8.c.(1) of this volume for additional guidance.

(2) Approval of an FCL or storage does not remove the requirement for a U.S. contractor on a USG-controlled installation in a foreign country to have the applicable export authorization, unless an exemption of the ITAR applies whereby the U.S. contractor is sending classified information or material overseas for U.S. contractor use only with no disclosure to a foreign person.

d. U.S. Contractor Operations Outside of the United States. With respect to such U.S. contractor operations, DSS will:

(1) Provide advice on industrial security to USG organizations and U.S. contractors that have employees assigned outside of the United States.

(2) Verify U.S. contractor PCLs and FCLs to foreign governments and NATO.

(3) Arrange a government-to-government channel for the secure transfer of classified information or material, provide advice and assistance in the preparation of security documentation, and assist in making arrangements with U.S. and foreign government security officials for transfers of classified information and material.

(4) Process requests for classified visits by employees of U.S. contractors, including verification of an export authorization or other need-to-know and providing the U.S. security assurance.

(5) Exercise oversight, in accordance with Paragraph 3.8.c.(1) of this volume and other provisions of this manual, of those U.S. contractor locations with an FCL for which DSS is the CSO on USG-controlled installations in a foreign country.

e. U.S. Contractor Employees Located on a Foreign Government or NATO-Controlled Facility or Installation.

(1) The foreign government's DSA or designee exercises oversight of U.S. contractor employees located on a foreign government of NATO-controlled facility or installation. Classified material to be used by U.S. contractor employees located at a foreign government installation, a foreign company (including foreign subsidiaries of U.S. parent companies), or a NATO installation in support of a foreign government or NATO contract must be transmitted via government-to-government channels to the foreign government or NATO in accordance with the provisions of this manual.

(2) Classified material will be handled by the recipient foreign government or NATO, in compliance with bilateral security agreements or United States Security Authority for NATO Affairs Instruction 1-07, as applicable. The host facility or installation will verify that the contractor employees comply with applicable host-nation rules and regulations.

12.18. NATO REQUIREMENTS.

a. General. The prime contract for a NATO program or project normally is awarded by a NATO production and logistics organization or a designated NATO program or project management office or agency. A NATO contract also may be awarded by a NATO research and development organization or a NATO Command. A NATO member nation may act as the lead nation for a NATO program or project, and thus award a NATO prime contract.

(1) Subcontracting under a NATO classified contract normally is handled in the same manner as classified U.S. contracts, in accordance with Section 6 of this volume; consent does not need to be obtained from the NATO contracting entity, unless the contract provides otherwise.

(2) U.S. contractors that hold a NATO contract will notify the NATO contracting entity and DSS, in writing, of the award of a subcontract.

b. Protection of NATO Information. United States Security Authority for NATO Affairs Instruction 1-07 sets forth the overall requirements for protection of NATO information. In the event of conflicts between this manual and United States Security Authority for NATO Affairs Instruction 1-07 for the protection of NATO information, DSS will refer the matter to OUSD(P) Director, ISP, with an information copy to the OUSD(I) CI&S, for resolution.

c. NATO Facility Security Clearance Certificate. In order for a U.S. company to bid on, negotiate, or perform on a NATO classified contract, the company must have or be sponsored for a U.S. FCL of at least the same classification level of the potential contract, in accordance with the provisions of Section 4 of this volume. DSS will issue a NATO FCL certificate if the U.S. contractor has the requisite U.S. FCL and its personnel requiring access to the NATO classified information possess the required level of U.S. PCL and have been briefed on NATO procedures.

d. Access to NATO Classified Information. Access to NATO classified information is authorized when the U.S. contractor employee has the requisite level of U.S. PCL and has been briefed on NATO security procedures. A NATO security clearance certificate validates the access authorization.

(1) A NATO personnel security clearance (NATO PCL) certificate is required for an employee to have access to NATO information classified NATO CONFIDENTIAL and above.

(2) Access to NATO classified information requires a final U.S. PCL at the equivalent level, except that an interim U.S. TS PCL is valid for access to NATO SECRET and NATO CONFIDENTIAL information. A PCL is not required for access to NATO RESTRICTED information; employees must, however, be informed of security requirements.

(3) DSS will issue a NATO PCL certificate for those cleared U.S. citizens requiring a NATO PCL certificate, including those who are employed by NATO civil and military bodies through NATO direct hire program in accordance with DoDI 5210.60.

(4) DSS will verify that U.S. cleared companies maintain records identifying all of their employees who have access to NATO information classified NATO CONFIDENTIAL and higher, using the format published on the DSS website at www.dss.mil.

e. Classification Guidance. DSS will provide assistance to the contractor in obtaining the necessary information from the NATO contracting entity, when classification guidance and security requirements have not been provided, or they are provided but are not adequate. Security classification guidance for a NATO classified contract normally will be provided by the contracting entity in the form of a NATO security aspects letter and security requirements checklist. For some large NATO programs, DSS will coordinate with OUSD(P) Director, ISP on the required program/project security instruction and SCG.

f. NATO Briefings to Cleared U.S. Contractor Personnel or DCMA Personnel. DSS will:

(1) Provide an initial NATO briefing to the contractor's FSO who will then be responsible for briefing other employees. The briefings must cover security requirements and the consequences of negligent handling of NATO classified information. When access is no longer required, personnel will be debriefed.

(2) Verify that U.S. contractors having access to NATO information classified NATO

CONFIDENTIAL and above provide their employees with an initial NATO security briefing and annual refresher briefings, and that the contractor maintains records of the annual briefings until the next briefing. Record retention requirements for debriefings of U.S. contractor employees are provided in DoD 5220.22-M and will be maintained for 2 years.

g. Safeguarding and Accounting for NATO Classified Information. NATO security policy requires that NATO classified information be safeguarded and accounted for as described in this paragraph.

(1) Receipts.

(a) Receipts are not required for NATO RESTRICTED or NATO CONFIDENTIAL information.

(b) DSS will verify that companies maintain such receipts for the receipt and dispatch of NATO SECRET and above information. A continuous chain of receipts is required for the receipt, internal distribution, destruction, and dispatch of COSMIC TS, NATO SECRET information, all ATOMAL information and any other accountable NATO classified information.

(2) Storage. DSS will verify that U.S. contractors store information classified NATO CONFIDENTIAL and above in the same manner as U.S. classified information of the equivalent level in accordance with Section 7 of this volume.

(a) NATO classified information will not be co-mingled with other classified information or material. Access by non-NATO briefed individuals must be prevented.

(b) NATO RESTRICTED information will be stored in a manner that precludes unauthorized access, such as a locked desk or locked file cabinet, or in the open in a secured room to which access is controlled to prevent unauthorized access to the information.

(3) Inventories.

(a) DSS will confirm that U.S. contractors with COSMIC TS, NATO SECRET, and all ATOMAL inventory the information annually as described in DoD 5220.22-M.

(b) An annual inventory of NATO SECRET information is not specifically mandated; NATO requires that NATO SECRET holdings be periodically reviewed to ensure proper accountability and control.

(c) NATO RESTRICTED and CONFIDENTIAL are not inventoried.

(4) Reproduction.

(a) COSMIC TS information will not be reproduced except in exceptional circumstances for mission essential purposes. When the originator has not provided the

necessary number of copies at the beginning of the program, project or contract and the exceptional conditions are met, the reproduction will be authorized by the Central United States Registry, which will provide guidance on accountability and control of the copies.

(b) Information classified NATO SECRET and below may be reproduced based on the strict need-to-know principle; procedures for safeguarding, accountability, and control of the original will apply to the copies; copy numbers will be applied to copies and a record will be maintained of the copies.

(c) NATO RESTRICTED and CONFIDENTIAL information may be reproduced as necessary for contract purposes, and copies will be safeguarded in the same manner as the original.

(5) Destruction. DSS will verify that U.S. contractors comply with destruction requirements described in DoD 5220.22-M.

(a) COSMIC TS information will be returned to a NATO registry or control point for destruction, which will be witnessed as provided for in DoD 5220.22-M.

(b) NATO CONFIDENTIAL and SECRET information will be destroyed by any means approved for the destruction of U.S. CONFIDENTIAL and SECRET information. The destruction of NATO SECRET information will be witnessed as provided for in DoD 5220.22-M.

(c) NATO RESTRICTED information may be destroyed in any manner that makes reconstruction reasonably difficult. Destruction certificates are required for all NATO classified documents except NATO CONFIDENTIAL.

(6) Records. DSS will verify that U.S. contractors comply with the records retention requirements for COSMIC TS information and NATO SECRET information as well as for the international transfer of NATO CONFIDENTIAL information as described in DoD 5220.22-M or in compliance with GCA specific records retention requirements.

h. International Transfers of Classified NATO Information. DSS will:

(1) Verify that U.S. contractors receive and send COSMIC TS, NATO SECRET, and all ATOMAL and other accountable information through the registry system. United States Security Authority for NATO Affairs Instruction 1-07 requires the establishment of a central distribution point for the receipt and distribution of accountable NATO documents. The central distribution point for the United States is the Central United States Registry, administered by the Department of the Army. NATO CONFIDENTIAL and RESTRICTED information will be transferred in the same manner as non-NATO FGI as described in paragraph 12.12 of this volume

(2) Follow the procedures at Paragraph 12.14 of this volume when approving the hand carriage plans of U.S. contractors for NATO classified information, except that DSS will issue

a NATO courier certificate to the hand carrier. NATO security authorities may authorize the hand carrying of NATO information classified NATO RESTRICTED and above by U.S. contractor employees across international borders when a demonstrated need exists.

(3) Verify that a U.S. contractor under DSS cognizance, if transmitting NATO information classified NATO RESTRICTED and above by IT or communication systems, has received formal approval by the NATO COMSEC authority or its designee that the confidentiality of the information will be protected by cryptographic methods and products.

i. Disclosure of U.S. Classified Information to NATO. When the disclosure or release of U.S. classified information is authorized for NATO, DSS will verify that the U.S. contractor has the required export authorization or written foreign disclosure authorization and appropriately marks the information as authorized for release to NATO.

j. NATO Visits. DSS will provide the required NATO PCL certificate and the U.S. security assurance to NATO security authorities for visits by U.S. contractor employees to NATO Headquarters, to NATO civil and military organizations, and to other cleared U.S. and foreign companies involved in a NATO classified program, project, or contract.

12.19. RECIPROCAL FILING OF CLASSIFIED PATENT APPLICATIONS.

a. Classified patent applications will be filed in accordance with DoDI 2000.03.

b. If the patent application involves a U.S. contractor under the NISP, DSS will:

(1) Upon receipt of a request from the foreign government and prior to the release of any classified information to the U.S. patent agent, provide the FCL status of the proposed U.S. patent firm.

(2) Process the agent for an appropriate FCL and notify the foreign government of the status of the clearance and the address of the responsible DSS field office if the agent either does not possess an FCL or the current clearance is at a lower level than required. See Paragraph 4.8.c.(14)(c) and Paragraph 7.4.a, of this volume for additional guidance on patent attorneys or patent firms.

c. After DSS has granted and confirmed the appropriate FCL, the foreign government and cleared U.S. patent agent may then transmit and receive the classified information through approved government-to-government channels in accordance with DoDI 2000.03 and this section.

d. If a requirement should arise involving a patent application at the TS level, the matter will be handled on an individual basis between the foreign government concerned and DSS.

SECTION 13: ASSOCIATED PROGRAMS OR INFORMATION

13.1. AA&E.

a. DSS will assess contractor compliance with DoD physical security requirements for the protection of sensitive AA&E, when requested in accordance with DoDD 5105.42 and DoDM 5100.76.

b. AA&E are designated as Security Risk Category (SRC) I-IV according to the risks involved with their relative utility, attractiveness, and availability to criminal elements. The description of each SRC, the minimum standards and criteria for the physical security of AA&E in the custody of DoD contractors is prescribed in DoDM 5100.76. The GCA will specifically prescribe any additional security requirements.

c. In accordance with the physical security requirements in DoDI 5100.76, the GCA will:

(1) Include requirements for the protection of conventional AA&E in the contract.

(2) Ensure that solicitations and contracts contain entry authority to enable the USG to conduct physical security surveys, inspections, and investigations.

(3) Ensure that the government activity designated as responsible for security surveys, inspections, and investigations receive timely notice of that designation and the relevant and governing portions of the contract.

d. AA&E not designated as SRC I-IV by DoDM 5100.76 will be protected and controlled in accordance with the contracting DoD GCA's prescribed minimum security requirements based on DoDM 5100.76 and included in the contract.

13.2. BIOLOGICAL SELECT AGENTS AND TOXINS (BSAT) BIOLOGICAL PERSONNEL RELIABILITY PROGRAM (BPRP). The BPRP is established to ensure the highest possible standards of individual reliability in personnel performing duties associated with BSAT. DoDI 5210.89 provides for minimum security standards for safeguarding BSAT.

13.3. CHEMICAL AGENT PERSONNEL RELIABILITY PROGRAM (CPRP). The CPRP is established to ensure the highest possible standards of individual reliability in personnel performing duties associated with chemical agents. DoDI 5210.65 provides minimum security standards for safeguarding chemical agents.

13.4. CLASSIFIED NATIONAL SECURITY INFORMATION PROGRAM FOR STATE, LOCAL, TRIBAL, AND PRIVATE SECTOR INFORMATION ENTITIES. E.O. 13549 established a classified national security information program designed to safeguard and govern access to classified national security information shared by the Federal Government with State, local, tribal, and private sector entities. As directed by E.O. 13549, the Department

of Homeland Security (DHS) published an implementing directive for uniform implementation of these standards, DHSD Classified National Security Information Program for State, Local, Tribal and Private Sector Entities.

13.5. COMSEC INFORMATION. COMSEC information is controlled and managed under a separate set of security standards and procedures from those that apply to other classified information in accordance with NSA/CSS Policy Manual 3-16.

a. COMSEC information may be provided to U.S. contractors with a valid need-to-know when:

(1) Electrical transmission of classified or sensitive unclassified national defense information is required among contractors or between contractors and the USG.

(2) The contractor is undertaking research, development, production, or testing of COMSEC equipment or of communications equipment interfacing with COMSEC equipment.

(3) The contractor is required to install, maintain, or operate accountable COMSEC equipment.

b. The NSA/CSS central office of record (COR) maintains records of all COMSEC material for COMSEC accounts under its purview. This includes COMSEC material that has been furnished to, generated, or obtained by those DoD contractors under the cognizance of the NSA/CSS COR.

c. DSS will:

c. (Added)(AF) When the Installation Commander provides oversight of on-installation cleared facilities, the Information Protection Office and the Cybersecurity Squadron will accomplish the tasks assigned to DCSA. (T-1)

(1) Provide a copy of DSS oversight visit results to the applicable COR when COMSEC material has been or potentially may be at risk.

(2) Notify the GCA of any security matter (incident report or FCL invalidation) that calls into question the protection of COMSEC material, and send a courtesy copy to the NSA/CSS COMSEC Incident Threat Office. The NSA/CSS COMSEC Incident Threat Office will then coordinate with the GCA and the Controlling Authority of any keying material involved.

(3) If requested by NSA/CSS, DSS will:

(a) Provide a COMSEC or Cryptographic Access briefing to the contractor's FSO.

(b) Conduct limited security reviews of contractor COMSEC accounts as part of the

regular, recurring security review process.

(c) Provide a copy of COMSEC security review results to the appropriate COR.

(d) Notify the COMSEC Incident Threat office and appropriate COR when COMSEC material is lost, tampered with, or accessed by unauthorized personnel.

d. The GCA will:

(1) Incorporate any contractor COMSEC security requirements that are in addition to DoD 5220.22-M into a DD Form 254.

(2) Request that the appropriate COR establish a contractor COMSEC account.

(2) (Added)(AF) In accordance with the DD Form 254 Instructions, a contractor COMSEC account is only required when the contractor must store accountable COMSEC material at their cleared facility in the performance of the contract. When contractor access to COMSEC information will occur at a government facility under the Air Force COMSEC account, the contractor will not be required to obtain a contractor COMSEC account.

(3) Verify with DSS that procedures have been established for the physical safeguarding of COMSEC materials and for the secure and efficient operation of a cryptosystem prior to release to the contractor.

(4) Provide written approval for subcontracting that requires the disclosure of classified COMSEC material.

(5) Provide approval and instructions to the contractor pertaining to the transmission of classified COMSEC material.

(6) Designate any contractor employees who are authorized to act as couriers for TS COMSEC material.

(7) Forward any unsolicited COMSEC system, equipment, development, study, or proposal submitted by a contractor to the Deputy National Manager for National Security Systems, NSA/CSS, Fort George G. Meade, Maryland 20755-6000, for evaluation and a determination as to whether or not it requires protection in the interest of national security.

(8) Notify their appropriate Command Authority and COR when DSS oversight visit results indicate COMSEC material has been or potentially may be at risk.

e. NSA/CSS will, when notified, take action based on Paragraph 13.5.c.(2) of this volume.

13.6. CNWDI. Due to the extreme sensitivity of CNWDI, access will be limited to the absolute

minimum number of persons who have a valid need-to-know. CNWDI is a DoD category of TS RD or SECRET RD. Access to and handling of CNWDI will be in accordance with DoDI 5210.02.

a. When CNWDI requirements involve a U.S. contractor, DSS will:

a. (Added)(AF) When the Installation Commander provides oversight of on-installation cleared facilities, the Information Protection Office will accomplish the tasks assigned to DCSA. (T-1)

(1) Provide an initial CNWDI briefing to the contractor's FSO.

(2) Maintain a record of contractor access to CNWDI.

(3) Verify contractor CNWDI access.

b. When CNWDI requirements involve a U.S. contractor, the GCA will:

(1) In accordance with Section 6 of this volume, notify DSS that access to CNWDI is required for contract performance.

(2) Ensure that the need-to-know principle is strictly enforced and that contractor personnel have been briefed on their responsibilities for handling CNWDI prior to disclosure.

(3) Ensure that classified material provided to U.S. contractors containing CNWDI is clearly marked as such.

(4) Provide written approval for transmission and disclosure of CNWDI among cleared companies.

13.7. CPI IDENTIFICATION AND PROTECTION. The GCA will include contractual terms requiring the company to protect CPI in accordance with DoDI 5000.02, DoDI 5200.39, Volume 3 of DoDM 5200.01 and Volume 4 of DoDM 5200.01.

13.8. CRADAS. DSS will consider a CRADA to be a legitimate USG requirement for an FCL, in accordance with Section 4 of this volume, if the non-federal party requires access to classified information and the terms of the CRADA are in accordance with DoDI 5535.8 and the applicable GCA's CRADA requirements.

13.9. DEFENSE TECHNICAL INFORMATION CENTER (DTIC)

a. In accordance with DoDD 5105.73, the DTIC is the central point within DoD for acquiring, storing, retrieving, and disseminating scientific and technical information to support the management and conduct of research, development, engineering, and study programs. Refer

to Volume 1 of DoDM 5200.01, for the transmission and repository requirements for security classification guides.

b. The GCA may authorize contractor use of DTIC services on the DD Form 254. The level of access granted to a contractor depends upon the classification of the contract to be registered with DTIC and the approval of the USG approving official A contracting officer, contracting officer's technical representative;, contracting officer's representative, program manager, or project manager may approve a contractor or contractor employee's request to register with DTIC and subsequently to have access to DoD controlled information while working on an official effort supporting a particular contract. For DTIC registration, go to www.dtic.mil/dtic/ and select registration.

13.10. IR&D EFFORTS. Contractors frequently use classified IR&D efforts to explore technological advancements and state-of-the-art improvements. DoDI 3204.01establishes policy and assigns responsibilities for the technical and business aspects of IR&D and bid and proposal activities.

a. The GCA for the contract under which classified information was originally provided to the contractor will continue to have jurisdiction over the information, even when such information has been incorporated into IR&D efforts.

b. With appropriate GCA authorized retention authority, cleared companies will be permitted to retain classified material generated in connection with their classified IR&D efforts for the duration of their FCL provided they have proper storage capability.

c. DSS will not continue an FCL for the sole purpose of retention of classified IR&D material without specific retention authority from the GCA having jurisdiction over the classified information. DSS may process a new FCL for a facility solely for the purpose of IR&D if a GCA certifies that the FCL is required for a government purpose and the contractor meets all other eligibility criteria in Section 3 of this volume.

13.11. INSTALLATION, BASE, OR FACILITY PHYSICAL ACCESS. Directive-type Memorandum 09-012, DoD 5200.08-R, and DoD Instruction 5200.08 or their successors provide the DoD policy for all individuals requiring physical access to DoD installations, bases, and facilities. These policies identify the standards for acceptable physical access control systems, authorized credentials to facilitate access, identity proofing and vetting for visitors, and a valid justification for entry.

13.12. NUCLEAR WEAPON PERSONNEL RELIABILITY PROGRAM (PRP). The PRP is established to ensure the highest possible standards of individual reliability in personnel performing duties associated with nuclear weapons and critical components. PRP policy is contained in DoDI 5210.42.

13.13. OPSEC

a. OPSEC policy is established in DoDD 5205.02E or its successor and implemented in DoD 5205.02-M or its successor.

b. Operational security essential to defense activities may be compromised whenever open sources (such as technical articles, press releases, National Technical Information Service publications, the Congressional Record, or contract awards) and detectable activities provide information that when compiled or analyzed is a detriment to U.S. interests.

c. If OPSEC requirements are necessary for a contract, the requiring organization and GCA, in accordance with the provisions of DoDD 5205.02E, will conduct an OPSEC review of the SOW prior to the release to contract bidders because the SOW, as a publicly released document, may reveal critical information or indicators of critical information. GCAs should work with their local OPSEC program managers and coordinators to identify OPSEC requirements for the scope of work to be performed and will determine security provisions for critical information if disclosed in the SOW.

d. The OPSEC program is applicable to NISP contractors when the GCA determines that additional safeguards are essential for specific contracts and imposes OPSEC as a contractual requirement in addition to the NISP.

e. The GCA will determine if OPSEC measures are required for performance on a contract. If OPSEC measures are required, the GCA will:

(1) Ensure that specific, detailed OPSEC requirements are incorporated into the solicitation, contract, subcontract, or addendum to enable the contractor's full understanding of any security requirements in excess of DoD 5220.22-M. Full understanding of these requirements is essential to ensure the contractor's ability to perform tasks and the government's ability to evaluate performance.

(2) Indicate on the DD Form 254, item 11j, that OPSEC requirements apply and provide specific details in block 14 or the appendix to ensure understanding. If specific details of the OPSEC requirements are in the SOW or other section of the contract documentation, then identify precisely where these requirements are included.

(3) Provide assistance to DSS when requested to ensure adequacy of security review efforts relating to OPSEC measures in accordance with Section 14 of this volume.

f. In accordance with DoDD 5205.02E and DoD 5205.02-M, DSS will:

f. (Added)(AF) When the Installation Commander provides oversight of on-installation cleared facilities, the Information Protection Office and the OPSEC Coordinator will accomplish the tasks assigned to DCSA. (T-1)

(1) As part of regularly scheduled security reviews, assess contractor compliance with the OPSEC requirements and contractually imposed countermeasures.

(2) Request GCA assistance with OPSEC reviews when deemed appropriate.

(3) Participate in and assist the GCA, when requested, with OPSEC surveys of cleared companies performing classified contracts and participating in the NISP.

13.14. RD AND FRD. RD and FRD are classified pursuant to the authority of section 2011 et seq., of Title 42, U.S.C. (also known and referred to in this volume as "The Atomic Energy Act of 1954, as amended". In its oversight role, DSS will assure that contractors performing on or in possession of RD and FRD must protect this type of material consistent with the provisions of DoD 5220.22-M.

13.15. TEMPEST COUNTERMEASURES.

a. In accordance with DoDI 8500.01, TEMPEST countermeasures will only be respectively in proportion to the threat of exploitation and the resulting damage to the national security if the information were to be obtained by a foreign intelligence organization. Contractors will only apply TEMPEST countermeasures if such special security requirements are specifically incorporated into a contract.

b. In accordance with DoDI 8500.01:

(1) The DSS will:

(1) (Added)(AF) When the Installation Commander provides oversight of on-installation cleared facilities, the Information Protection Office and the Cybersecurity Squadron will accomplish the tasks assigned to DCSA. (T-1)

(a) Incorporate a review of the contractor's compliance with the TEMPEST countermeasures imposed by the contract as part of the regular security review process.

(b) Request GCA assistance with the TEMPEST aspect of security reviews, when needed.

(2) The GCA will:

(a) Perform threat assessment and vulnerability studies to determine if classified information may be exposed to TEMPEST collection.

(b) Identify in writing any TEMPEST countermeasures that may be required and incorporate such requirements into the classified contract.

(c) Provide a copy of TEMPEST contract requirements to DSS.

(d) Provide approval for prime contractors to impose TEMPEST countermeasures in subcontracts, only if warranted in proportion to the threat of exploitation and the resulting damage to the national security if the information were to be obtained by a foreign intelligence organization.

13.16. PROTECTION OF MISSION CRITICAL FUNCTIONS TO ACHIEVE TRUSTED SYSTEMS AND NETWORKS.

a. DoDI 5200.44 establishes policy to minimize the risk that DoD's warfighting mission capability will be impaired due to vulnerabilities in system design, sabotage or subversion of a system's mission critical functions or critical components by foreign intelligence, terrorists, or other hostile elements. DoDI 5200.44 directs action in accordance with the supply chain risk management strategy of the National Security Presidential Directive 54/Homeland Security Presidential Directive 23 DoDI 5200.44.

b. The Defense MicroElectronics Activity (DMEA) Trusted Access Program Office (TAPO) facilitates and administers the contracts and agreements with industry to provide the USG with long term access to sate of the art integrated circuit design and manufacturing services for specialized USG applications, both classified and unclassified. TAPO has the overall security cognizance for the Trusted Foundry program. The TAPO can be contacted at https://www.dmea.osd.mil/Tapo/contactUs.html.

c. DMEA serves as the DoD Trusted Foundry Program Manager. DMEA accredits suppliers that have implemented a trusted flow in the areas of integrated circuit design, aggregation, broker, mask manufacturing, foundry, post processing, packaging/assembly or test services. DMEA provides microelectronics support to other government entities and suppliers and helps to coordinate policy for use by accredited suppliers.

d. TAPO sponsorship of FCLs is an essential element of the accreditation requirements for trusted suppliers. TAPO keeps DSS apprised of any special provisions required for inspections when the trusted supplier is under DSS security cognizance.

SECTION 14: SECURITY REVIEWS AND CONTINUING SECURITY ASSURANCE ACTIVITY

14.1. SECURITY REVIEWS.

a. DSS' role as the NISP CSO for the DoD is to provide GCAs with assurances that contractors are eligible for access to classified information and have systems in place to properly safeguard the classified information in their possession and to which they have access. The continuing process of providing those assurances to the GCAs depends upon DSS knowledge of the security practices and procedures established and maintained by the contractor facilities. One of the primary means of obtaining that knowledge is through the recurring industrial security review process. Security review efforts should be accomplished as a collaborative effort with emphasis on problem solving. Recognizing that the security review process imposes a burden on the contractor, the time from entrance briefing (initiation date) until exit briefing (completion date) will not ordinarily exceed 30 days.

b. If the Commander of a USG-controlled installation has security cognizance of a contractor facility on the installation, the Commander will conduct security reviews in accordance with the provisions of this section. The Commander will provide completed security reviews and continuing security assurance updates to DSS in accordance with the provisions of Paragraph 3.8.c.(3) of this volume to allow DSS to continue to verify the FCL and, as applicable, the safeguarding capability of the cleared on-base contractor facility.

b. (Added)(AF) Information Protection Offices will maintain up-to-date information regarding security reviews for on-installation cleared facilities in the SAF/AAZ designated repository. (T-1) Information Protection Offices will provide completed security review reports to the local DCSA field office with a copy sent to dss-isfo.mbx.qao-goco@mail.mil. (T-1)

c. DSS will conduct:

c. (Added)(AF) When the Installation Commander maintains oversight of on-installation cleared facilities, the Information Protection Office will conduct: (T-1)

(1) An onsite visit to approve safeguarding at contractor facilities as soon as possible after granting the FCL when the sponsor includes a requirement for safeguarding of classified information in the DD Form 254 or associated documentation.

(2) A security review at all cleared facilities within 15 months of the FCL being granted.

d. Frequency of reviews, after the initial security review set forth in Paragraph 14.1 of this volume, will be consistent with the principle of risk management in accordance with E.O. 12829 and this manual.

(1) Since the passage of time between security reviews is one element of risk, there is a

baseline inspection frequency (see Paragraph 14.1.d.(2) of this volume for a description of the process to defer, accelerate or continue the baseline inspection frequency based on risk management methodology):

(a) Facilities authorized to possess classified material and all facilities cleared under FOCI mitigation mechanisms will be reviewed every 12 months.

(b) All other facilities will be reviewed every 18 months.

(c) Parent organizations that have executed formal exclusion resolutions in accordance with Paragraph 4.10.b of this volume will be reviewed in conjunction with their cleared subsidiaries' security reviews. DSS will conduct onsite reviews of excluded parents when there are identified risks that merit an onsite review.

(2) DSS will establish a risk management methodology to be used in determining which security reviews may be deferred, or, as circumstances warrant, accelerated or continued on the baseline frequency set forth in Paragraphs 14.1.d.(1)(a) through 14.1.d.(1)(c) of this volume. A GCA may request an accelerated review if the GCA is aware of circumstances that indicate its classified information may be at risk. DSS will reassess this risk management methodology and provide the current version to OUSD(I) CI&S prior to the beginning of each fiscal year.

(2) (Added)(AF) When the Installation Commander maintains oversight of on-installation cleared facilities, security reviews will not be deferred. (T-1). The Installation Commander will follow the schedule identified in Paragraphs 14.1.d.(1) and 14.1.d.(2) of this volume to complete reviews. (T-0)

e. DSS will notify the relevant GCA and Component industrial security office of the results of its security reviews of cleared contractor facilities when marginal or unsatisfactory ratings are issued. For reviews determined marginal or unsatisfactory, DSS will notify those offices of the basis for the rating, the schedule for rectification, and the subsequent results. DSS will advise the contractor corporate headquarters of its security review results across a contractor's cleared facilities when the results reflect a significant systemic issue or a serious issue that would benefit from corporate awareness and interest. DSS will advise of positive ratings upon the request of the GCA.

e. (Added)(AF) When the Installation Commander maintains oversight of on-installation cleared facilities, the Information Protection Office will notify DCSA of security reviews resulting in marginal or unsatisfactory ratings in accordance with Paragraph 3.8.c.(5)(a)6. through MAJCOM information protection channels. (T-1)

f. (Added)(AF) Self-Inspections and Self-Assessments for visitor groups. Installation Commanders will include contractor integrated visitor groups within their self-inspection programs in accordance with AFI 16-1404. (T-1) Information Protection Offices and other security relevant program areas (e.g., Cybersecurity Squadron, AFOSI, etc.) will evaluate independent visitor groups separate from their government sponsor. (T-1) Evaluation criteria will be based upon requirements identified in AFI 16-1404 and local

security policy communicated to the contractor. Information Protection Offices and other security relevant program areas will evaluate independent visitor groups at a frequency based on risk management principles, not to exceed 24 months. (T-3) Contracting officers will ensure a requirement for contractors to support these activities is included in appropriate contracts. (T-1)

g. (Added)(AF) Information Protection Offices shall utilize the Enterprise Protection Risk Management (EPRM) tool as the designated system for recording and aggregating key elements of self-inspections within their respective organizations as well as other organizations being supported through host tenant support agreements, memoranda of understanding, memoranda of agreement, or supplements. (T-1) The EPRM tool will provide information to Commanders useful in the risk management decision process while also achieving requirements to internally assess the health of the security program.

14.2. SCOPE OF SECURITY REVIEWS.

a. Security reviews constitute an assessment of the systems that comprise the contractor's security program with an emphasis on actions taken to ensure that previously identified issues have been fully corrected. In conducting its oversight, DSS will focus on interviews of cleared employees and the use of IS to process classified information.

b. In accordance with Paragraph 14.1 of this volume, DSS or the Commander will assure that security reviews address, but not be limited to:

(1) KMP Changes. Changes in KMP (e.g., new KMP, retired or different KMP, non-U.S. KMP).

(2) Exclusion Resolutions. Ensure that resolutions have been executed as appropriate and are effective.

(3) FCL. Review changes in corporate structure or ownership to determine the potential impact on the contractor's security clearance in accordance with the FCL eligibility and retention factors in Section 3 of this volume.

(4) FOCI. Review SF 328 information concerning FOCI and ensure that it is still current (see Volume 3 of this manual for detailed procedures for review of FOCI factors).

(5) Security Education. Review the contractor's system for providing initial and recurring security education to its cleared employees and adequacy of the information provided. Determine if cleared employees are aware of requirements of DoD 5220.22-M that relate to their jobs. Determine that the contractor has a program for briefing its employees about actual or potential insider threats, suspicious contacts and the technology collection efforts by other countries.

(6) Visits. Review the contractor's program for sending cleared employees on visits requiring access to classified information at other locations and procedures for processing

incoming visitors requiring access to classified information during their visit.

(7) Access Authorizations, to Include Need for PCLs.

(a) Verify the process used to review the SF 86 "Questionnaire for National Security Positions" for adequacy and completeness.

(b) Verify that the privacy of the individuals completing the SF 86 has been maintained.

(c) Validate the need for PCLs and LAAs.

(d) Verify that the contractor is using JPAS or the successor DoD system of record for access and eligibility determinations in accordance with required procedures.

(8) Classification. Determine if the contractor has the appropriate classification guidance from the customer. If the contractor has no current or prospective classified contracts, provide information relating to administrative termination of the contractor's security clearance.

(9) Use of Subcontractors. Ensure that the FCL of the subcontractors has been verified and that a DD Form 254 containing appropriate classification guidance has been provided.

(10) Adverse Information Reporting. Verify that the contractor has a program for reporting adverse information about its cleared employees. Evaluate the effectiveness of the program at the contractor. Also, verify that the contractor established and maintains an insider threat program in accordance with DoD 5220.22-M. Evaluate the effectiveness of the insider threat program at the contractor and consider the size and complexity of the contractor in assessing its implementation.

(11) Self-inspection. Ensure that a program is in place for recurring, formal self-inspections and that it has sufficient scope, depth, and frequency related to the activity, information, and conditions, and receives management support in execution and remedy.

(12) Threat and CI. In accordance with the provisions of this manual, conduct review and evaluations with understanding of threat to the facility and its information and the CI analysis and conclusions regarding nature and sources of risk for the facility. Based on identified threats to the facility, assess whether the security program and performance provide acceptable countermeasures and how such countermeasures could be improved.

(12) (Added)(AF) When Installation Commanders retain oversight of on-installation cleared facilities, the supporting AFOSI detachment coordinates with the Information Protection Office to provide counterintelligence support to the security review. (T-1)

(13) Contractors Possessing Classified Material On-site. For contractors that possess classified material on-site at the contractor location, additional elements apply (this list is not

all- inclusive):

(a) Hosting Classified Visits. Review of the contractor's procedures for establishing need-to-know and precluding unauthorized access to classified information.

(b) Classified Material Controls. Review of the contractor's procedures for handling and storing classified material to determine if they are effective in deterring and detecting unauthorized access.

(c) IS. Review of the contractor's procedures for processing classified information on approved IS. Specifically target systems with modifications or those approved by the contractor via self-approval authority.

(c) (Added)(AF) When Installation Commanders retain oversight of on-installation cleared facilities, the Cybersecurity Squadron coordinates with the Information Protection Office to provide support regarding the review of classified information systems in the custody of the contractor. (T-1)

(d) Reproduction and Disposition. Review of the contractor's system for classified disposition and destruction methods to ensure that only authorized material is retained. Also ensure their system provides for destruction by appropriately cleared employees and, for TS information, includes a witness.

(e) International Involvement. Determine if the contractor has any international involvement in classified programs and that appropriate measures are in place and implemented for any foreign visitors and for any foreign national employees. (See Paragraph 12.16 of this volume).

(14) Areas of Special Emphasis

(a) Review of FFs. Initial reviews of FFs include verification of registration with the DoS, determination of any problems with the local customs and Transportation Security Administration security offices, and contact with SDDC for any relevant information they may have about the FF. The FF security review includes a review of export licenses and approved transportation plans.

(b) Review of Commercial Carriers. The review of a commercial carrier includes the HOF as well as the specific terminals authorized to handle SECRET shipments. The approved transportation plan provides the basis for the review.

(c) Review of Excluded Parents. The parent corporation of a cleared subsidiary that has been excluded from access to classified information, in accordance with Paragraph 4.10.b of this volume, will be reviewed in conjunction with their cleared subsidiaries' security reviews. DSS will conduct onsite reviews of excluded parents when there are identified risks that merit an onsite review. DSS will emphasize FOCI reporting during such reviews and in other contacts with the excluded parent.

c. DSS will rate the contractor's security posture at the conclusion of each security review. This rating provides a description of the contractor's effectiveness in protecting classified information. DSS will periodically reassess its methodology for assigning ratings and provide the current version to OUSD(I) CI&S prior to the beginning of each fiscal year. These ratings are described as:

(1) Superior. The superior security rating is reserved for contractors that have consistently and fully implemented the requirements of DoD 5220.22-M in an effective fashion, resulting in a security posture of the highest caliber compared with other cleared companies of similar size and complexity. A contractor assigned a rating of superior must have documented and implemented procedures that heighten the security awareness of contractor employees and must foster a spirit of cooperation within the security community. This rating also requires that a sustained high level of management support must be present for the security program. This rating cannot be assigned if any serious security issues or vulnerabilities that may be indicative of a systemic issue were found during the most recent DSS security review. For contractors with complex operations, minor administrative results from the most recent DSS security review will not preclude a rating of superior.

(2) Commendable. The commendable security rating is assigned to contractors that have fully implemented the requirements of DoD 5220.22-M in an effective fashion, resulting in an exemplary security posture compared with other contractors of similar size and complexity. This rating denotes a security program with strong management support, the absence of any serious security issues or vulnerabilities that may be indicative of systemic issues, and only minor administrative results.

(3) Satisfactory. The satisfactory security rating is the most common rating and denotes that a contractor's security program is in general conformity with the basic requirements of this manual. This rating can be assigned even if there were vulnerabilities requiring corrective action in one or more of the security program elements within the contractor's overall security program. Depending on the circumstances, a satisfactory rating can be assigned even if there were isolated serious vulnerabilities during the security review.

(4) Marginal. The marginal security rating is assigned when a contractor's security program is not in general conformity with the basic requirements of DoD 5220.22-M. This rating signifies a serious vulnerability in one or more security program areas that could contribute to the eventual compromise of classified information if left uncorrected. The contractor's size, the extent of classified activity, and the inherent nature of the identified security problem(s) should be carefully considered before this rating is assigned. The industrial security representative (ISR) will conduct a required compliance review within 120 days after the security review that led to the marginal security rating, to assess the effectiveness of any actions taken by the contractor to correct the vulnerabilities that led to the marginal rating. DSS will also notify the GCA of the marginal rating as described in Paragraph 14.1.d of this volume.

(5) Unsatisfactory.

(a) The unsatisfactory security rating is the most serious adverse security rating. An unsatisfactory rating is assigned when circumstances and conditions indicate that the contractor has lost, or is in imminent danger of losing, its ability to adequately safeguard the classified information in its possession, or to which it has access. This rating is appropriate when the security review results indicate that the contractor can no longer credibly demonstrate that it can be depended upon to preclude the disclosure of classified information to unauthorized persons.

(b) When the issuance of an unsatisfactory rating is considered, DSS must notify the security and CI points of contact for those GCAs that have a classified contract with the contractor of the intended unsatisfactory rating, along with the nature and scope of the vulnerabilities, the specific contracts affected, and to the extent known, the action taken by the contractor to eliminate the danger of compromise, the contractor's plan to correct the situation, and the projected completion date.

(c) The ISR must conduct a compliance review within 30 days of the review or event that led to the unsatisfactory rating to assess the effectiveness of corrective actions taken. If the contractor refuses to take corrective action and is unwilling or has consistently demonstrated an inability to protect classified information, DSS may invalidate or revoke the FCL issued to the contractor based on an unsatisfactory rating.

(d) When DSS invalidates or revokes a contractor FCL, in accordance with the provisions of Paragraph 4.15 or 4.17 respectively of this volume, DSS will update the FCL status for verification by the Components or their GCAs, as applicable, in accordance with the provisions of Paragraph 4.3.a of this volume.

d. DSS will convey the assigned rating in an exit briefing with the contractor's senior management official, if available, and the FSO. In addition, DSS will:

(1) Notify the corporate director of security, if there is one, when there is a marginal or unsatisfactory rating at a branch or subsidiary facility. Notice to the GCA(s) will occur in accordance with Paragraph 14.1.d of this volume.

(2) Identify any corrective actions to be taken by the contractor that require senior management attention, if applicable.

(3) Provide a written report of vulnerabilities to the FSO.

(4) Provide formal written notification to the contractor's senior management official of the overall results of the security review as well as an assessment of the contractor's security posture signed by the DSS Field Office Chief.

(5) Send the formal written notification as soon as possible, but not later than 30 days after the conclusion of the security review.

14.3. COMPLIANCE SECURITY REVIEW.

a. A compliance security review is required when a contractor's security posture has been rated as marginal or unsatisfactory. The purpose of the compliance security review is to confirm that the contractor has taken the necessary steps to implement specific security procedures and to ensure that countermeasures are effective in protecting the classified information provided to the contractor. The DSS ISRs conducting the review must be satisfied that no further erosion of the security program will occur and that contractor management will continue to provide the support necessary for an effective security program.

b. If the compliance security review reveals that a contractor with a marginal rating has failed to take the appropriate action to correct problem areas, the security effectiveness rating may remain as marginal and another compliance security review will be scheduled within 30 days. The marginal rating can be downgraded to unsatisfactory if conditions remain marginal.

14.4. CLOSEOUT SECURITY REVIEW.

a. When a contractor has not participated in a classified procurement effort for a 12-month period, has no immediate prospects for obtaining a classified contract, and the GCA has not authorized retention of classified material or provided justification for retention of the inactive FCL, the FCL will be administratively terminated and a closeout review conducted. The closeout security review is conducted to ensure appropriate disposition of all classified material and that the contractor has accomplished all other necessary close-out actions.

b. A closeout security review is not required for a contractor that does not possess classified material at the contractor location, except at the discretion of DSS.

14.5. SECURITY REVIEW REPORT. DSS will maintain records of the results in accordance with its records management manual and NARA, Records Disposition Authority, N-1 446-0905, "Industrial Security Case Files," after the completion of the review. Those commanders who exercise security cognizance of cleared facilities on USG controlled installations will maintain records of results in accordance with their applicable Component record management manual and their approved records retention schedule from the NARA. The Commanders provide those results and updates to DSS, in accordance with their records management manuals and the provisions of Paragraph 14.1 of this volume. A report of each security review will be compiled detailing information collected pertaining to each security system applicable to the contractor's security program. (See Appendix 14 A of this volume for a listing of information that the report should contain, as a minimum.)

14.6. ADVICE AND ASSISTANCE. DSS will advise the contractor and GCAs to achieve and maintain an effective security program. DSS will be responsive to the contractor's changing contractual or program requirements and other influences impacting a contractor's security program.

APPENDIX 14A: SECURITY REVIEW REPORT

14A.1. DSS or the Commander, as applicable, will compile a report of each security review detailing information collected pertaining to each security system applicable to the contractor's security program. When a Commander or his or her designee acts as the DGR at a contractor location based on security cognizance responsibility in accordance with Paragraph 3.8.c.(3) of this volume, DSS will review the Commander's DGR records to ensure compliance with industrial security policy. DSS will provide a report to the Commander or designee and provide training in areas that are deficient or not in accordance with industrial security policy.

14A.2. The report will contain, at a minimum:

a. The amount of time expended on the security review.

b. Core identifying information pertaining to the contractor.

c. Basic information about the FCL and any FOCI mitigation instruments.

d. Detailed information pertaining to any vulnerability as a result of the security review and corrective action required.

e. A brief summary description of each of the contractor's security systems (e.g., personnel, information, physical, insider threat).

f. Information that describes the size and complexity of the contractor's security program, such as:

(1) Numbers and types of classified contracts and programs performed.

(2) The number of cleared employees by clearance level as well as the total number of all employees (both cleared and uncleared).

(3) The volume and media (e.g., documents, hardware, and software) of classified material held by the contractor.

(4) Numbers and types of storage containers and facilities.

(5) The numbers and types of IS.

(6) Any FOCI.

(7) International involvement.

(a) Foreign commercial classified contract information.

(b) Export authorizations.

(c) FGI.

(d) TCPs.

(e) Program or project security instructions.

(f) Foreign visitors.

(g) Security education/support/oversight for employees at overseas locations.

(h) Identification by name of the individual acting as the U.S. DGR.

(8) Special programs (depending upon sensitivity may be stored elsewhere).

(9) Other special requirements imposed by the GCA(s) on the contractor.

(10) Applicable threat assessments (which may be stored separately depending upon sensitivity and protection requirements).

(11) The rating of the contractor's security posture.

GLOSSARY

G.1. ACRONYMS.

AA&E	arms, ammunition, and explosives
(Added)(AF) AFI	**Air Force Instruction**
(Added)(AF) AFMAN	**Air Force Manual**
(Added)(AF) AFOSI	**Air Force Office of Special Investigations**
(Added)(AF) AFOSI PJ	**Air Force Office of Special Investigations, Office of Special Projects**
(Added)(AF) AFPD	**Air Force Policy Directive**
(Added)(AF) AFSAC	**Air Force Security Assistance and Cooperation Directorate**
AO	authorizing official
BPRP	Biological Personnel Reliability Program
BSAT	biological select agents and toxins
CAC	Common Access Card
CFR	Code of Federal Regulations
CI	counterintelligence
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
CNWDI	critical nuclear weapon design information
COMSEC	communication security
COR	Central Office of Record
CPI	critical program information
CRADA	cooperative research and development agreement
CPRP	Chemical Agent Personnel Reliability Program
CSA	cognizant security agency
CSO	cognizant security office
DCS	direct commercial sales
(Added)(AF) DCSA	**Defense Counterintelligence and Security Agency**
DDTC	Directorate of Defense Trade Controls
DGR	designated government representative
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DMEA	Defense MicroElectronics Activity
DNI	Director of National Intelligence

DoD CAF	DoD Consolidated Adjudications Facility
(Added)(AF) DoDAAC	**Department of Defense Activity Address Code**
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
DOE	Department of Energy
DOHA	Defense Office of Hearings and Appeals
DoS	Department of State
(Added)(AF) DRU	**Direct Reporting Unit**
DSA	designated security authority
DSCA	Defense Security Cooperation Agency
DSP	Department of State form
DSS	Defense Security Service
DTIC	Defense Technical Information Center
DTS	Defense Transportation System
DVO	Defense Visits Offices
E.O.	Executive Order
EPLS	Excluded Parties Lists System
(Added)(AF) EPRM	**Enterprise Protection Risk Management**
FBI	Federal Bureau of Investigation
FCL	facility security clearance
FCLA	facility security clearance assurance
FF	freight forwarders
FGI	foreign government information
FIE	foreign intelligence entity
FMS	foreign military sales
(Added)(AF) FOA	**Field Operating Agency**
FOCI	foreign ownership, control, or influence
FRD	Formerly Restricted Data
FSO	facility security officer
FVS	foreign visit system
GCA	Government Contracting Activities
GC DoD	General Counsel of the Department of Defense
GSA	General Services Administration
HOF	home office
ICD	Intelligence Community Directive

IR&D	independent research and development
IS	information system
ISFD	Industrial Security Facilities Database
ISL	industrial security letters
ISOO	Information Security Oversight Office
ISR	industrial security representative
IT	information technology
JPAS	Joint Personnel Adjudication System
JV	joint venture
KMP	key management personnel
LAA	limited access authorization
LLC	limited liability company
(Added)(AF) LOA	**Letter of Offer and Acceptance**
(Added)(AF) MAJCOM	**Major Command**
MDCO	Military Department Counterintelligence Organization
MFO	multiple facility organization
MOU	memorandum of understanding
NATO	North Atlantic Treaty Organization
NATO PCL	North Atlantic Treaty Organization personnel security clearance
(Added)(AF) NCCS	**National Industrial Security Program Contract Classification System**
NISP	National Industrial Security Program
NISPPAC	National Industrial Security Program Policy Advisory Committee
(Added)(AF) NISS	**National Industrial Security System**
NSA/CSS	National Security Agency/Central Security Service
OCA	original classification authority
OMB	Office of Management and Budget
(Added)(AF) OPR	**office of primary responsibility**
OPSEC	operations security
OS	operating system
OUSD(I) CI&S	Office of the Under Secretary of Defense for Intelligence, CI and Security
OUSD(P)	Office of the Under Secretary of Defense for Policy
OUSD(P) Director, ISP	Office of the Under Secretary of Defense for

	Policy Director, International Security Programs, Defense Technology Security Administration
PCL	personnel security clearance
PCLSA	personnel security clearance assurance
(Added)(AF) PIEE	**Procurement Integrated Enterprise Environment**
PRP	Personnel Reliability Program
PSI	personnel security investigation
(Added)(AF) PII	**personally identifiable information**
(Added)(AF) PSO	**Program Security Officer**
RD	Restricted Data
RFV	requests for visits
ROM	repair, overhaul, or maintenance
(Added)(AF) SAF/AA	**Administrative Assistant to the Secretary of the Air Force**
SAM	System for Award Management
SAP	Special Access Program
SAPCO	Special Access Program Central Office
SCG	security classification guide
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SDDC	Surface Deployment and Distribution Command
SecDef	Secretary of Defense
SETA	security education training and awareness
SF	standard form
SRC	security risk category
SOR	statement of reason
SOW	statement of work
TAPO	Trusted Access Program Office
TCP	technology control plan
TS	Top Secret
U.S.C.	United States Code
(Added)(AF) USD(A&S)	**Under Secretary of Defense for Acquisition and Sustainment**
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
USD(I)	Under Secretary of Defense for Intelligence

USD(P)	Under Secretary of Defense for Policy
(Added)(AF) USD(R&E)	**Under Secretary of Defense for Research and Engineering**
USG	U.S. Government
U.K.	United Kingdom
VAL	visit authorization letter
(Added)(AF) VROC	**Vetting Risk Operations Center**
WHS	Washington Headquarters Services

G.2. DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

access. Defined in DoD 5220.22-M.

(Added)(AF) activity security manager. Defined in AFI 16-1404.

adverse information. Defined in DoD 5220.22-M.

ATOMAL. Defined in Volume 2 of DoDM 5200.01.

authorized person. Defined in DoD 5220.22-M.

bilateral security agreements. Collectively, the General Security Agreements and General Security of Information Agreements (GSOIAs), which pertain to the safeguarding of all classified information; the General Security of Military Information Agreements, which pertain to the safeguarding of classified information generated by or for the DoD or which is under its jurisdiction or control; and the industrial security annexes to the General Security Agreements, GSOIAs, and General Security of Military Information Agreement s.

carrier. Defined in Defense Transportation Regulation 4500.9-R.

carve-out. Defined in DoDD 5205.07.

classification. Defined in Volume 1 of DoDM 5200.01.

classified contract. Defined in DoD 5220.22-M.

classified information. Defined in Joint Publication 1-02.

classified visit. Defined in DoD 5220.22-M.

classifier. Defined in DoD 5220.22-M.

clear. Rendering an administrative determination that, from a security viewpoint, an individual or legal entity is eligible for access to classified information of a certain category (and all lower

categories).

cleared commercial carrier. Defined in DoD 5220.22-M.

cleared employees. Defined in DoD 5220.22-M.

closed area. Defined in DoD 5220.22-M.

CNWDI. Defined in DoDI 5210.02.

collateral information. All national security information classified CONFIDENTIAL, SECRET, or TS under the provisions of an E.O. for which special systems of compartmentation (such as SCI or SAP) are not formally required.

colleges and universities. Defined in DoD 5220.22-M.

company. Defined in DoD 5220.22-M.

compromise. Defined in DoD 5220.22-M.

COMSEC. Defined in Joint Publication 1-02.

CONFIDENTIAL. Defined in DoD 5220.22-M.

contractor. Defined in DoD 5220.22-M.

consultant. An individual who is under contract to provide professional or technical assistance to a contractor in a capacity requiring access to classified information.

contracting officer. Defined in DoD 5220.22-M.

corporation. A legal entity, organized and existing under the laws of one of the 50 States, the District of Columbia, or one of the organized U.S. territories, with articles of incorporation generally filed with the government of the State in which the corporation is established, governed by a set of bylaws and owned by its stockholders who elect a board of directors to manage the company.

COSMIC TS: Defined in Volume 2 of DoD 5200.01.

counterintelligence. Defined in DoDD 5240.02.

courier. Defined in DoD 5220.22-M.

CPI. Defined in DoDI 5200.39.

CSA. Defined in DoD 5220.22-M.

CSO. Defined in DoD 5220.22-M).

declassification. Defined in DoD 5220.22-M).

defense articles. Defined in parts 120-130 of Title 22, CFR, also known as the ITAR.

defense industrial base. Defined in Joint Publication 1-02.

derivative classification. Defined in DoD 5220.22-M.

DGR. An individual serving as a DoD or other USG transmittal authority overseeing the transfer of classified defense articles and technical data through official government-to-government channels, or through other channels agreed upon by both governments.

document. Defined in E.O.13526.

downgrade. Defined in DoD 5220.22-M.

DSA. The senior government official responsible for establishing security policy and procedures for international programs. The DoD DSA is the OUSD(P) Director, ISP.

empowered official. Defined in parts 120-130 of Title 22, CFR, also known as the ITAR.

EPLS. Defined in subpart 9.4 of the FAR.

escort. Defined in DoDM 5220.22-M.

espionage. Defined in Joint Publication 1-02.

FCL. Defined in DoD 5220.22-M.

FCLA. A written certification by government industrial security authorities, which certifies the FCL level and storage capability level of a facility under the USG or applicable foreign government's security jurisdiction.

federal information systems. Defined in CNSSI 4009.

FF. Defined in DoD 5220.22-M.

FGI. Defined in E.O. 13526.

foreign intelligence entity. Defined in Joint Publication 1-02.

FMS. Defined in Joint Publication 1-02.

FMS case implementing agency. Defined in DSCA Manual 5105.38.

foreign national. Defined in DoD 5220.22-M.

franchise. A business model that involves a grantor licensing its name, product, trademark, or methods and business formats to an individual or business organization.

FRD. Defined in DoDI 5210.02.

GCA. An element of a Component designated and delegated by the Component head or designee with broad authority regarding acquisition functions to include the appropriate resources and personnel (e.g., contracting officers or their designees, program managers, program offices, and security personnel) with appropriate security education and training, in accordance with paragraph 2.7.c of this volume.

government-to government-channels. The transfer of classified material using official government transmission or transportation channels (e.g., the U.S. Transportation Command's Defense Courier Division (TCJ3-C); the Defense Transportation System; the Diplomatic Pouch System).

government-to-government principle. The principle that the export or foreign disclosure of classified material will be based on a decision that the classified information involved is authorized for disclosure to the government or international organization of the intended recipient or end-user.

government-to-government transfer. The transfer of classified material using official government transmission or transportation channels (e.g., the U.S. Transportation Command's Defense Courier Division (TCJ3-C)); the Defense Transportation System; the Diplomatic Pouch System) or through other channels that have been agreed to in writing by both governments.

grantor. One who grants a license or franchises to other individuals or business organizations to use the name, administrative support, method of operation or style of the grantor in a specific area.

Indian tribe. Defined in section 479a of Title 25, U.S.C., also known as "The Indian Reorganization Act, as amended."

information. Defined in DoD 5220.22-M.

Insider Threat Program Senior Official. Defined in DoD 5220.22-M.

international organization. An entity established by recognized governments pursuant to an international agreement which, by charter or otherwise, is able to acquire and transfer property, make contracts and agreements, obligate its members, and pursue legal remedies.

invalidation. An administrative action that renders a contractor ineligible to receive or access additional classified material except that information necessary for completion of essential contracts as determined by appropriate GCAs.

IR&D efforts. Defined in DoDI 5535.8.

JV. A business undertaking by a combination of two or more persons or business entities that perform or act jointly in a specific endeavor, such as the negotiation for, or performance of, a contract.

joint venturers. The shareholders, members, or partners, depending on the business structure of the JV, who enter into a business undertaking to perform or act jointly for a specific endeavor or contract.

LLC. Both a business entity and an investment vehicle that seeks to provide some of the benefits of both the corporation and the partnership with ownership typically divided pro rata according to the members' investments. Regardless of the degree of ownership, a member of the LLC has the legal power to bind the LLC in the making of contracts and many other undertakings. The same authority to bind the entire enterprise applies to LLC managers. This legal authority exists whether or not the manager is also a member, and whether the manager has been authorized by the LLC to enter into the transaction. In most cases, the LLC is operated by a management board selected by the members; however, it may be operated by the members themselves. The management board may be made up of members, hired (non-member) management personnel, or a combination of both.

licensee. An individual or business organization that holds or is issued a license or franchise from a grantor to use the grantor's name, administrative support, method of operation or style in a specific area.

MDCO. Defined in DoDD 5240.06.

meetings at which classified information is disclosed. Applies to a conference, seminar, symposium, exhibit, convention, training course, or other such gathering during which classified information is disclosed. These provisions do not apply to meetings related to a specific contract or project, including pre-proposal or pre-award meetings, and post-award briefings conducted by the GCA; nor do they apply to meetings conducted by cleared companies and attended by contractor personnel directly involved in the performance of a contract or project. Volume 3 of DoDM 5200.01 provides the requirements for such meetings.

MFO. Defined inDoD 5220.22-M.

national security authority. Defined in DoDD 5100.55.

NATO PCL certificate. Defined in United States Security Authority for NATO Affairs Instructions 1-07.

NATO SECRET. Defined in Volume 2 of DoDM 5200.01.

NISPPAC. Defined in E.O. 12829.

OCA. Defined in E.O. 13526.

OPSEC. Defined inDoDD 5205.02E.

original classification. Defined in E.O. 13526.

partnership. An association of two or more individuals (or other business entities) who have agreed to do business together as owners for profit. No separate legal entity is created.

PCL. Defined in DoD 5220.22-M.

PCLSA. A written certification by USG or applicable foreign government industrial security authorities, which certifies the PCL level or eligibility for a PCL at a specified level for their citizens. The assurance is used, in the case of the United States, to give an LAA to a non-U.S. citizen, provided all other investigative requirements are met.

personally identifiable information. Defined in DoDD 5200.11.

prime contractor. Defined in DoD 5220.22-M.

program/project security instruction. Defined in Chapter 9 of the Office of the Deputy Under Secretary of Defense for Policy Integration and Chief of Staff Handbook, "International Programs Security.

RD. Defined in DoDI 5210.02.

receipt. A written or digitally signed acknowledgment of having received a specified item, information, freight, or documents.

relevant authority. Defined in CNSSI 4005.

safeguarding. Defined in E.O. 13526 for protection of classified information or DoDD 5400.11 for protection of personally identifiable information.

SAM. A Federal Government-owned and operated free website (www.sam.gov) that consolidates the capabilities of other systems used in the federal procurement and awards processes, (e.g., the former EPLS for contractors debarred or suspended from federal procurements).

SAP. Defined in E.O. 13526.

SCG. Defined in Volume 1 of DoDM 5200.01.

SCI. Defined inJoint Publication 1-02.

security assurance. A written confirmation, requested by and exchanged between governments, that contains the following elements: verification of the PCL level of the providing government's citizens or nationals; a statement by a responsible official of the providing government that the recipient of the information is approved by the government for access to information of the security classification involved on behalf of the government; and an obligation that the government will ensure compliance with any security agreement or other security requirements specified by the USG. The security assurance usually will be in a request for visit authorization or with courier orders or a transportation plan; but is not related to the PCLSA.

security clearance. Defined in DoDM 5200.02.

security-in-depth. Defined in DoD 5220.22-M.

sole proprietorship. The simplest type of business structure; a business owned by one individual who is liable for the debts and other liabilities incurred in the operation of the business.

special category system. Tactical, embedded, data acquisition, legacy or special purpose IS requiring an alternative set of controls not readily available in typical systems since some IS are incapable of alteration by users and are designed and implemented to provide a very limited set of predetermined functions. These systems are characterized by some common features. First and most importantly, there are no general users on the system; and second, there is no user code running on the system. In addition, if an IS meets the criteria of a legacy system upgrading the systems in order to meet the baseline security controls may outweigh the benefit of the additional control and continued technological enhancements. Examples include some data acquisition systems and some other special purpose test type systems, such as those embedded as an integral element of a larger system that are used to perform or control a specific function (such as control systems or weapons systems) concurrently with the design and development of the system.

TEMPEST. Defined in Joint Publication 1-02.

temporary help supplier. A subcontractor who dispatches personnel on his or her payroll to perform work on the premises of a GCA or another contractor.

vulnerability. An identified weakness in a contractor's security program that indicates non-compliance with the requirements of DoD 5220.22-M that could be exploited to gain unauthorized access to classified information or information systems accredited to process classified information.

REFERENCES

Code of Federal Regulations, Title 5 Code of Federal Regulations, Title 22 Code of Federal Regulations, Title 32 Code of Federal Regulations, Title 36

Committee on National Security Systems Instruction 1253, "Security Categorization and Control Selection for National Security Systems," March 27, 2014[1]

Committee on National Security Systems Instruction 4001, "Controlled Cryptographic Items," May 7, 2013

Committee on National Security Systems Instruction 4005, "Safeguarding COMSEC Facilities and Materials," August 22, 2011[2]

Committee on National Security Systems Instruction 4009, "National Information Assurance Glossary," April 2015[3]

Committee on National Security Systems Policy 8, "National Policy Governing the Release and Transfer of US Government Cryptologic National Security Systems, Technical Security Material, Information, and Techniques to Foreign Governments and International Organizations," August 2012[4]

Committee on National Security Systems Policy 18, "National Policy on Classified Information Spillage," June 2006[5]

Committee on National Security Systems Policy 22, "Cybersecurity Risk Management," August 2016[6]

Defense Logistics Manual 4000.25, Volume 6, "Logistics Systems Interoperability Support Services," current edition[7]

Defense Security Cooperation Agency Manual 5105.38, "Security Assistance Management Manual (SAMM)," current edition[8]

Defense Transportation Regulation 4500.9-R, "Defense Transportation Regulation," current edition

"Department of Defense Foreign Clearance Guide," current edition[9]

[1] Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm.
[2] Available to authorized users of the SECRET Internet Protocol Router Network at http://www.iad.nsa.smil.mil/resources/library/.
[3] Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm.
[4] Available to authorized users of the SECRET Internet Protocol Router Network at http://www.iad.nsa.smil.mil/resources/library/.
[5] Available at https://www.cnss.gov/CNSS/issuances/Policies.cfm.
[6] Available at https://www.cnss.gov/CNSS/issuances/Policies.cfm.
[7] Available at http://www.dla.mil/HQ/InformationOperations/DLMS/elibrary/manuals/v6/.
[8] Available at http://www.samm.dsca.mil/listing/esamm.
[9] Available at https://www.fcg.pentagon.mil/fcg.cfm.

Department of Homeland Security, "Classified National Security Information Program for State, Local, Tribal and Private Sector Entities Implementing Directive", February 2012[10]

Deputy Secretary of Defense Memorandum, "DoD Central Adjudications Facilities Consolidation," May 3, 2012

Deputy Secretary of Defense Memorandum, "Training in International Security and Foreign Disclosure Support to International Programs," October 22, 1999

Director of Central Intelligence Directive 6/1, "Security Policy for SCI and Security Policy Manual," March 1, 1995

Director of National Intelligence Memorandum, "Delegation of Authority for Director of Administration and Management to Determine Sensitive Compartmented information Eligibility at the Department of Defense Consolidated Central Adjudication Facility," October 22, 2012

Directive-type Memorandum 09-012, "Interim Policy Guidance for DoD Physical Access Control," December 8, 2009, as amended

Directive Type Memorandum 15-002, "Policy Guidance for the Processing of National Interest Determinations (NIDs) in Connection with Foreign Ownership, Control, or Influence (FOCI)," February 11, 2015

DoD Directive 5100.55, "United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN)," February 27, 2006

DoD Directive 5105.42, "Defense Security Service (DSS)," August 3, 2010, as amended DoD

Directive 5105.73, "Defense Technical Information Center (DTIC)," May 2, 2013

DoD Directive 5111.1, "Under Secretary of Defense for Policy (USD(P))," December 8, 1999

DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and

Logistics (USD(AT&L))," December 9, 2005, as amended

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," October 24, 2014, as amended

DoD Directive 5145.01, "General Counsel of the Department of Defense (GC DoD)," December 2, 2013, as amended

DoD Instruction 5145.03, "Oversight of the DoD Personnel Security Programs," January 10, 2013

DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012 DoD

Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010

DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014

[10] Available at http://www.dhs.gov/xlibrary/assets/mgmt/mgmt-classified-national-security-program-implementation-directive.pdf.

DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992

DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005

DoD Directive 5240.02, "Counterintelligence," March 17, 2015

DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, as amended

DoD Directive 5220.6, "Defense Industrial Personnel Security Clearance Review Program," January 2, 1992, as amended

DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014, as amended DoD

Instruction 2000.03, "International Interchange of Patent Rights and Technical Information," January 17, 2006

DoD Instruction 3204.01, "DoD Policy for Oversight of Independent Research and Development (IR&D)," August 20, 2014

DoD Instruction 3305.13, "DoD Security Education, Training, and Certification," February 13, 2014

DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015

DoD Instruction 5025.01, "DoD Issuances Program," August 1, 2016, as amended

DoD Instruction 5100.76, "Safeguarding Sensitive Conventional Arms, Ammunition, and Explosives (AA&E)," February 28, 2014

DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," April 21, 2016

DoD Instruction 5200.02, "DoD Personnel Security Program (PSP)," March 21, 2014, as amended

DoD Instruction 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)," December 10, 2005

DoD Instruction 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)," May 28, 2015

DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012

DoD Instruction 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)," February 6, 2013

DoD Instruction 5210.02, "Access to and Dissemination of Restricted Data and Formerly Restricted Data," June 3, 2011

DoD Instruction 5210.42, "DoD Nuclear Weapons Personnel Reliability Assurance Program (PRP)," April 27, 2016

DoD Instruction 5210.65, "Minimum Security Standards for Safeguarding Chemical Agents," January 19, 2016

DoD Instruction 5210.60, "Security Clearance Program for U.S. Citizens Employed Directly By the North Atlantic Treaty Organization (NATO)," December 4, 2005

DoD Instruction 5210.89, "Minimum Security Standards for Safeguarding Biological Select Agents and Toxins," January 19, 2016

DoD Instruction 5220.22, "National Industrial Security Program (NISP)," March 18, 2011 DoD Instruction 5535.8, "DoD Technology Transfer (T2) Program," May 14, 1999

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014

DoD Manual 5100.76, "Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives," April 17, 2012

DoD Manual 5105.21, Volume 1, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security," October 19, 2012

DoD Manual 5105.21, Volume 2, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security," October 19, 2012

DoD Manual 5105.21, Volume 3, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities," October 19, 2012

DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012

DoD Manual 5200.01, Volume 2, "DoD Information Security Program: Marking of Classified Information," February 24, 2012, as amended

DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended

DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)," February 24, 2012

DoD Manual 5200.02, "Procedures for the DoD Personnel Security Program (PSP)," April 3, 2017

DoD Manual 54007.07, DoD Freedom of Information Act (FOIA) Program Collections," June 30, 2014

DoD Manual 5205.07, Volume 1, "DoD Special Access Program Security Manual: General Procedures," June 18, 2015

DoD Manual 5205.07, Volume 2, "DoD Special Access Program Security Manual: Personnel Security," November 24, 2015

DoD Manual O-5205.07, Volume 3, "DoD Special Access Program Security Manual: Physical Security," April 23, 2015

DoD Manual 5205.07, Volume 4, "DoD Special Access Program Security Manual: Marking," October 10, 2013

DoD Manual 5220.22, Volume 3, "National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)," April 17, 2014

DoD 5205.02-M, "DoD Operations Security (OPSEC) Program Manual," November 3, 2008

DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, as amended

DoD 5200.08-R, "Physical Security Program," April 9, 2007, as amended DoD 5400.11-R, "DoD Privacy Program," May 14, 2007

DoD 7750.07-M, "DoD Forms Management Program Procedures Manual," May 7, 2008, as amended

DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections," June 30, 2014

Executive Order 10865, "Safeguarding Classified Information within Industry," February 20, 1960, as amended

Executive Order 12829, "National Industrial Security Program," January 6, 1993, as amended

Executive Order 12968, "Access to Classified Information," August 2, 1995, as amended

Executive Order 13467, "Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information," June 30, 2008, as amended

Executive Order 13526, "Classified National Security Information," December 29, 2009

Executive Order 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," August 18, 2010

Executive Order 13764, "Amending the Civil Service Rules, Executive Order 13488, and Executive 13467 To Modernize the Executive Branch-Wide Governance Structure and processes for Security Clearances Suitability and Fitness for Employment and Credentialing, and Related Matters, January 17, 2017

Federal Acquisition Regulation, current edition

Intelligence Community Directive 700 "Protection of National Intelligence," June 7, 2012

Intelligence Community Directive 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to SCI and Other Controlled Access Program Information," October 1, 2008

Intelligence Community Directive 705, "Sensitive Compartmented Information Facilities (SCIF)," May 26, 2010

Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current edition

Memorandum of Understanding Between the Federal Bureau of Investigation and the Department of Defense Governing Information Sharing, Operational Coordination, and Investigative Responsibilities, August 2, 2011[11]

National Archives and Records Administration, Records Disposition Authority, N-1 446-09-5, "Industrial Security Facility Case Files," May 20, 2010[12]

[11] Available upon request to authorized users from the OUSD(I) CI&S Directorate, ODDI(I&S), Room 3C915, 5000 Defense Pentagon, Washington D.C. 20301-5000.

[12] Copy is available at http://www.archives.gov/records-mgmt/rcs/schedules/departments/ department-of-defense/defense-agencies/rg-0446/n1-446-09-005_sf115.pdf.

National Disclosure Policy-1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," October 1, 1988[13]

National Institute of Standards of Technology Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," Revision 1, February 2010[14]

National Security Agency/Central Security Service Policy Manual 3-16, "Control of Communications Security (COMSEC) Material," January 23, 2015[15]

National Security Presidential Directive 54/Homeland Security Presidential Directive 23, "Comprehensive National Cybersecurity Initiative," January 8, 2008[16]

Office of the Deputy Under Secretary of Defense for Policy Integration and Chief of Staff Handbook, "International Programs Security," current edition[17]

Office of Management and Budget Memorandum, "Reciprocal Recognition of Existing Personnel Security Clearances," December 12, 2005

Office of Management and Budget Memorandum M-06-21, "Reciprocal Recognition of Existing Personnel Security Clearances," July 17, 2006

Public Law 112-74, "Consolidated Appropriations Act, 2012," December 23, 2011

Public Law 112-199, "Whistleblower Protection Enhancement Act of 2012," November 27, 2012

Security Executive Agent Directive (SEAD) 4, National Security Adjudicative Guidelines June 8, 2017

Treaty Between the Government of the United States of America and the Government of the Australia Concerning Defense Trade Cooperation, September 5, 2007[18]

Treaty Between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland Concerning Defense Trade Cooperation, June 21, 2007[19]

Underwriter Laboratories 2050, "Standard for National Industrial Security Systems for the Protection of Classified Materials," current edition[20]

---

[13] Provided to designated disclosure authorities on a need-to-know basis from the Office of the Deputy Under Secretary of Defense for Policy Integration and Chief of Staff to the Under Secretary of Defense for Policy.

[14] Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37rl.pdf.

[15] Available to authorized users at www.iad.gov/cor.

[16] This classified document is available through OASD(HD&ASA) to users with the appropriate clearance based on need to know.

[17] Available at http://www.discs.dsca.mil/_pages/resources/default.aspx?section=publications&type=ips

[18] Available at http://www.pmddtc.state.gov.

[19] Available at http://www.pmddtc.state.gov.

[20] Available at www.ul.com/contact. Government agencies with a role as a Cognizant Security Agency or Cognizant Security Office may obtain this reference without charge.

Under Secretary of Defense for Intelligence Memorandum, "Minimum Requirements for Interim Eligibility to Access Secret and Confidential Classified Information," January 27, 2014[21]

United States Security Authority for NATO Affairs Instruction 1-07, "Implementation of NATO Security Requirements," 2007[22]

Under Secretary of Defense for Intelligence Memorandum, "Clarification of Overseas Protection Requirements for Classified Information, May 20, 2016[23]

United States Code, Title 5, Section 552 (also known as the "Freedom of Information Act"), as amended

United States Code Appendix 3, Title 18, Section 1 et.seq. (also known as "The Classified Information Procedures Act, as amended")

United States Code, Title 25 (also known as "The Indian Reorganization Act, as amended")

United States Code, Title 42, Section 2011 (also known as "The Atomic Energy Act of 1954, as amended")

United States Code, Title 50

(Added)(AF) Secretary of Defense Memorandum*, Renaming the Defense Security Service as the Defense Counterintelligence and Security Agency*, 20 June 2019

(Added)(AF) OUSD(I) Memorandum*, Use of the National Industrial Security Program Contract Classification System*, 8 February 2018

(Added)(AF) OUSD(I) Memorandum*, Clarification of Clearance Requirements for Access to Investigative and Adjudicative Relevant Data*, 27 June 2019

(Added)(AF) OUSD(A&S) Memorandum*, Use of National Industrial Security Program Contract Classification System*, 19 October 2018

(Added)(AF) AFI 16-701*, Management, Administration and Oversight of Special Access Programs*, 18 February 2014

(Added)(AF) AFI 16-1404*, Air Force Information Security Program*, 29 May 2015

(Added)(AF) AFI 33-332*, Air Force Privacy and Civil Liberties Program*, 12 January 2015

(Added)(AF) AFI 33-360*, Publications and Forms Management*, 1 December 2015

(Added)(AF) DoDM 5200.02_AFMAN16-1405*, Air Force Personnel Security Program*, 1 August 2018

[21] Available upon request from the OUSD(I) CI&S Directorate, ODDI(I&S), Room 3C915, 5000 Defense Pentagon, Washington D.C. 20301-5000.

[22] Reference may be obtained from the Central U.S. Registry.

[23] Available upon request from the OUSD(I) CI&S Directorate, ODDI(I&S), Room 3C915, 5000 Defense Pentagon, Washington D.C. 20301-5000.

(Added)(AF) AFMAN 17-1301, *Computer Security (COMPUSEC)*, 10 February 2017

(Added)(AF) AFMAN 31-113, *Installation Perimeter Access Control (FOUO)*, 2 February 2015

(Added)(AF) DoDM 5400.07_AFMAN33-302, *Freedom of Information Act Program*, 27 April 2018

(Added)(AF) AFI 14-403, *Sensitive Compartmented Information, Security and Intelligence, Surveillance, and Reconnaissance Systems Cybersecurity and Governance*, 3 September 2019

(Added)(AF) AFMAN 33-363, *Management of Records*, 1 March 2008

(Added)(AF) AFPD 16-14, *Security Enterprise Governance*, 31 December 2019

(Added)(AF) AFPD 71-1, *Criminal Investigations and Counterintelligence*, 1 July 2019

(Added)(AF) *DSS Assessment and Authorization Process Manual (DAAPM), Version 2*, 6 May 2019