

**BY ORDER OF THE  
SECRETARY OF THE AIR FORCE**

**AIR FORCE INSTRUCTION 31-601**

**22 NOVEMBER 2000**



**AIR EDUCATION AND TRAINING COMMAND  
Supplement 1**

**21 AUGUST 2001**

**Security**

**INDUSTRIAL SECURITY PROGRAM  
MANAGEMENT**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**NOTICE:** This publication is available digitally on the AFDPO WWW site at:  
<http://afpubs.hq.af.mil>.

---

OPR: HQ USAF/XOFI (Mr Dan Green)

Certified by: HQ USAF/XOF (Brigadier General  
James M. Shames)

Supersedes AFI 31-601, 1 April 1996

Pages: 40

Distribution: F

---

This instruction implements Air Force Policy Directive (AFPD) 31-6, Industrial Security. It provides guidance for implementing the National Industrial Security Program. Use this instruction with DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), DOD 5220.22-R, Industrial Security Regulation, and DOD 5200.1-R, Information Security Program Regulation and changes thereto. Maintain and dispose of all records created as a result of processes prescribed in this instruction in accordance with AFMAN 37-139, Records Disposition Schedule. HQ USAF/XOF is delegated approval authority for revision of this AFI.

---

**(AETC) AFI 31-601, 22 November 2000, is supplemented as follows:**

This supplement does not apply to the Air National Guard or the Air Force Reserve Command. Maintain and dispose of records created as a result of prescribed processes in accordance with AFMAN 37-139, *Records Disposition Schedule* (will become AFMAN 33-322, Volume 4).

### **SUMMARY OF REVISIONS**

**This document is substantially revised and must be completely reviewed.**

It aligns its guidance with the revised Air Force Policy Directive (AFPD) 31-6, Industrial Security. Revisions include renumbering the chapters; updating office symbols and publication references; requiring the identification of government information and sensitive resources that require protection in classified contract documents; mandating the integration of on-base contractor operations into the installation information security program per AFPD 31-6; requiring the execution of a security agreement with contractors that perform contractual services on Air Force installations and require access to classified and gives installation commanders the discretionary authority to also require the execution of an security agreement

with on-base contractors that require access to sensitive unclassified information or frequent "entry" to the installation; clarifying responsibilities and procedures for processing National Interest Determinations (NIDs); requiring a review of the DD Form 254, Contract Security Classification Specification, at two year intervals; requiring subcontractors that perform contractual services on Air Force installations to execute a Visitors Group Security Agreement (VGSA) when execution is required per this instruction; requiring contractors that use government automated information systems (AIS) to undergo a background investigation prior to AIS usage; and eliminating the requirement to use the DD Form 696, Industrial Security Inspection Report. (NOTE: As used in this publication, the term "security review" is not synonymous nor does it negate the "security and policy review" requirement of AFI 35-101, Air Force Public Affairs Policies and Procedures. The term "sensitive unclassified information" refers to information identified in a classified contract that has been marked "For Official Use Only (FOUO)" per DOD 5200.1-R, Information Security Program, and is exempt from release under the Freedom of Information Act (FOIA)).

<b>Chapter 1— GENERAL PROVISIONS AND REQUIREMENTS</b>	<b>5</b>
1.1. Policy. ....	5
1.2. Purpose. ....	5
1.3. Scope. ....	5
1.4. Submitting Interpretation and Waiver Requests. ....	5
1.5. Authority and Responsibilities. ....	5
1.6. Program Implementation and Administration. ....	6
1.7. Public Release of Information. ....	8
1.8. Reporting Requirements. ....	9
<b>Chapter 2— SECURITY CLEARANCES</b>	<b>12</b>
2.1. Facility Security Clearances (FCLs). ....	12
2.2. Contractors with Foreign Ownership, Control or Influence (FOCI). ....	12
2.3. Contractor Personnel Security Clearances (PCLs). ....	13
2.4. Processing Trustworthiness Determinations. ....	14
2.5. Reciprocity. ....	14
<b>Chapter 3— SECURITY TRAINING AND BRIEFINGS</b>	<b>15</b>
3.1. Security Training Requirements. ....	15
3.2. Security Briefing/Debriefing Requirements. ....	15
<b>Chapter 4— SECURITY SPECIFICATIONS AND GUIDANCE</b>	<b>16</b>
4.1. Issuing Security Classification Guidance. ....	16
4.2. DD Form 254, Contract Security Classification Specifications. ....	16

4.3. Reviewing and Certifying the DD Form 254. ....	16
4.4. Distribution of the DD Form 254. ....	17
4.5. Visitor Group Security Agreement (VGSA). ....	17
<b>Chapter 5— SAFEGUARDING</b>	<b>19</b>
5.1. Designation of On-Base Visitor Groups. ....	19
5.2. Integrated Visitor Group. ....	19
5.3. Cleared Facility. ....	19
5.4. Intermittent Visitors. ....	19
5.5. On-Base Contract Completion or Termination. ....	19
<b>Chapter 6— OVERSIGHT REVIEWS AND REPORTING REQUIREMENTS</b>	<b>20</b>
6.1. Conducting Industrial Security Reviews (SRs). ....	20
6.2. Conducting Information Security Program Reviews. ....	21
<b>Chapter 7— VISITS AND MEETINGS</b>	<b>23</b>
7.1. Installation Visitors. ....	23
7.2. Visitor Groups. ....	23
7.3. Contractor Visits to Air Force Installations. ....	23
7.4. Air Force Visits to Contractor Facilities. ....	23
<b>Chapter 8— SUBCONTRACTING</b>	<b>24</b>
8.1. Prime Contractor's Responsibilities. ....	24
8.2. Subcontractor Responsibilities. ....	24
<b>Chapter 9— AUTOMATED INFORMATION SYSTEM (AIS) SECURITY</b>	<b>25</b>
9.1. Automated Information Systems (AIS) Accreditation. ....	25
<b>Chapter 10— SPECIAL REQUIREMENTS</b>	<b>27</b>
10.1. Special Access Program. ....	27
10.2. Sensitive Compartmented Information. ....	27
<b>Chapter 11— INTERNATIONAL SECURITY REQUIREMENTS</b>	<b>28</b>
11.1. Procedures for Contractor Operations Overseas. ....	28
11.2. Disclosure of Information to Foreign Visitors/Interests. ....	28
11.3. Documentary Disclosure of Information to a Foreign Entity. ....	28
11.4. Foreign Visits ....	28

<b>Chapter 12— OTHER APPLICABLE SECURITY GUIDANCE</b>	<b>29</b>
12.1. Security Plans, Procedures, Operating Instructions and Training Mate .....	29
12.2. Applicability of Other Security Program Requirements. ....	29
<b>Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION</b>	<b>30</b>
<b>Attachment 2 (Added-AETC)—INSTRUCTIONS FOR COMPLETING A BASIC DD FORM 254</b>	<b>34</b>
<b>Attachment 3 (Added-AETC)—INSTRUCTIONS FOR COMPLETING A TASK ORDER DD FORM 254</b>	<b>40</b>

## Chapter 1

### GENERAL PROVISIONS AND REQUIREMENTS

**1.1. Policy.** It is Air Force policy to identify in its classified contracts (DD Form 254, **Contract Security Classification Specification**) [DOD 5220.22-R] specific government information (regardless of classification, sensitivity, physical form, media or characteristics) and sensitive resources, which must be protected against compromise and or loss while entrusted to industry.

**1.2. Purpose.** This instruction implement Executive Order 12829, *National Industrial Security Program*, DOD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, and DOD 5220.22-R, *Industrial Security Regulation (ISR)* and AFPD 31-6, *Industrial Security*. It assigns functional responsibilities and establishes a system of review that identifies outdated, inappropriate and unnecessary contractual security requirements. It outlines and provides guidance for establishing on-base integrated contractor visitor groups.

**1.3. Scope.** The security policies, requirements and procedures identified in this instruction are applicable to Air Force personnel and on-base DOD contractors performing services under the terms of a properly executed contract and associated security agreement or similar document, as determined appropriate by the installation commander (IC).

**1.4. Submitting Interpretation and Waiver Requests.** Submit requests regarding the interpretation, clarification and/or waiving of requirements stipulated in Air Force Policy Directive (AFPD) 31-6, *Industrial Security* and this instruction through command Information Security Program Manager (ISPM) channels to HQ USAF/XOFI, 1340 Air Force Pentagon, Washington, D.C., 20330-1340.

#### **1.5. Authority and Responsibilities.**

1.5.1. The Secretary of Defense (SECDEF) is the Cognizant Security Agency (CSA) for the Department of Defense (DOD). The SECDEF has designated the Defense Security Service (DSS) as the Cognizant Security Office (CSO) for DOD. DSS oversees security for cleared contractor facilities located off-base and on-base when so requested by the installation commander, in writing.

1.5.2. The Administrative Assistant to the Secretary of the Air Force (SAF/AA) is designated the Air Force Senior Security Official responsible for ensuring implementation of the Industrial Security Program.

1.5.3. Headquarters United States Air Force, Director of Security Forces, Information Security Division, (HQ USAF/XOFI) is responsible for industrial security policy development, interpretation, administration and program oversight.

1.5.4. The Assistant for Federal Acquisition Regulation (FAR) System, Deputy Assistant Secretary (Contracting), Assistant Secretary (Acquisition), (SAF/AQC) is responsible for formulating and interpreting contracting policy and issuing supplemental guidance to the FAR. The contracting office (CO) is responsible for coordinating contractual changes and modifications with Air Force contractors.

1.5.5. Headquarters United States Air Force, Director of Intelligence, Surveillance, and Reconnaissance (HQ USAF/XOI) is responsible for Sensitive Compartmented Information (SCI) policy, when applicable to Air Force (AF) awarded contracts.

1.5.6. Headquarters United States Air Force, Director of Communications and Information (HQ USAF/SC) is responsible for formulating and overseeing implementation of automated information systems (AISs) security policy, and disseminating communications security (COMSEC) and emission security (EMSEC) guidance, when applicable to AF awarded contracts. HQ USAF/SC also formulates and disseminates guidance pertaining to DOD Regulation 5400.7/AF Supplement, *Freedom of Information Act Program*. Referenced publication addresses the handling, marking and protection of sensitive unclassified and “For Official Use Only (FOUO)” information.

1.5.7. Headquarters United States Air Force, DCS/Air & Space Operations, Director of Intelligence, Surveillance and Reconnaissance (HQ USAF/XOI), 1480 Air Force Pentagon, Washington D.C., 20330-1480, formulates policy and disseminates guidance pertaining to AFD 10-11, *Operations Security (OPSEC)*, requirements, when applicable to an AF awarded contract.

1.5.8. The Secretary of the Air Force, Office of Public Affairs Security and Review Division (SAF/PAS) formulates policy and disseminates guidance pertaining to the clearance and release of information to the public, in any form.

1.5.9. The IC or designated designee is responsible for authorizing and/or granting DOD contractors access to the installation and for providing appropriate security supervision over the on-base contractor operation and its personnel.

## 1.6. Program Implementation and Administration.

1.6.1. The IC will:

1.6.1.1. Designate on-base contractor operations that require access to classified information as an intermittent visitor, visitor group, or cleared facility.

1.6.1.2. Execute a VGSA with all contractor operations located on Air Force installations that require or will have access to classified information. This provision may also be extended to include other contractors that perform contractual services on the installation and require or have access to sensitive unclassified information or those that require routine or infrequent “entry” to the installation in the performance of other types of contracts, services or maintenance.

**1.6.1.2. (AETC)** AETC installation commanders will establish visitor groups for AETC activities that require contract support. On-base contractor cleared facilities are not authorized for AETC activities.

1.6.1.3. Ensure NISPOM or equivalent security procedures are implemented for contractor operations supporting classified efforts within the confines of the installation.

1.6.1.4. Designate the installation ISPM (see AFI 31-401, Information Security Program Management) as the authority to perform industrial security program oversight for on-base contractor operations, unless unique or special operational circumstances warrant the use of the DSS.

**1.6.1.4. (AETC)** In AETC, the information security program manager (ISPM) is responsible for supervision and oversight of onbase integrated visitor group contractors. The HQ AETC/DOYI special security office (SSO) or the local SSO is responsible for the supervision and oversight of sensitive compartmented information (SCI) contracts issued by AETC contracting organizations. The SSO is also responsible for supervision and oversight of collateral classified information maintained in SCI storage areas. DoD 5200.1-R, *Information Security Program Regulation*, and AFI 31-401, *Managing the Information Security Program*, will be used to provide oversight of

collateral classified information. The Director of Security Forces (HQ AETC/SF) is the ISPM for contracts that directly support HQ AETC.

1.6.1.5. Ensure security reviews are conducted on those on-base contractor operations designated as a “cleared facility,” when determined by the IC. In these instances, DSS must be notified that the Air Force will retain “security oversight” for the on-base contractor operations.

1.6.2. Air Force Activity (System, Program or Project Manager) will:

1.6.2.1. Initiate procurement requests and identify program unique security requirements in solicitations and contract documents.

1.6.2.2. Draft and incorporate program specific security classification guidance into the DD Form 254, **DOD Contract Security Classification Specification**.

**1.6.2.2. (AETC)** AETC organizations will notify the ISPM as soon as they know a contractor will require access to classified information during contract performance. The office developing the contract requirements will coordinate with the ISPM to ensure security classification guidance is provided by use of a DD Form 254, **DoD Contract Security Classification Specification**. Other security requirements will be incorporated into the statement of work (SOW) or performance work statement (PWS). The ISPM will review all DD Forms 254 before they are submitted to the procuring contracting officer (PCO). HQ AETC/SF is the ISPM for all industrial security matters, including coordination on DD Form 254 issued by headquarters activities.

1.6.2.3. Coordinate contractual security specifications with the contracting office and responsible security discipline, office of primary responsibility (OPR) or functional.

1.6.2.4. As a minimum, review the DD Form 254 biennially and revise or modify the security classification guidance, as appropriate.

1.6.2.5. Work in concert with the CO, ISPM, security program disciplines and/or functional OPRs to develop the VGSA.

**1.6.2.5. (AETC)** Provide the project or program manager a sample AETC visitor group security agreement (VGSA) to use for developing or modifying security procedures to meet local unique requirements. The sample VGSA can be found on the HQ AETC/SFI web page. The program manager, project manager, or functional area chief (FAC) will prepare DD Forms 254 with the advice and assistance of the ISPM and the contracting office. See instructions for completing DD Form 254 at [Attachment 2 \(Added\)](#) and [Attachment 3 \(Added\)](#), this supplement.

1.6.3. Contracting Officers will:

1.6.3.1. Implement the NISPOM by incorporating specific security clauses into (classified/unclassified) contracts and solicitations as outlined in the Federal Acquisition Regulation (FAR) and supplementation thereto.

1.6.3.2. Negotiate all contractual agreements, modifications, changes and revisions with contractors.

1.6.3.3. Initiate and/or implement other actions as outlined in the FAR, DFARS, AFFARS, NISPOM and ISR relative to the administration of the industrial security program.

1.6.4. The Defense Security Service (DSS) will accomplish the following tasks per DOD 5220.22-M, NISPOM and DOD 5220.22-R, ISR:

1.6.4.1. Administer the National Industrial Security Program (NISP) in accordance with national and DOD policy.

1.6.4.2. Establish and maintain a network of automated systems which provide real-time personnel security clearance (PCL) and facility security clearance (FCL) data on DOD contractors and their employees.

1.6.4.3. Assume industrial security program oversight responsibility for on-base cleared facilities at the request of the IC.

1.6.5. Information Security Program Manager (ISPM) will:

1.6.5.1. Oversee and administer the industrial security program on behalf of the IC.

**1.6.5.1. (AETC)** The ISPM will develop a memorandum of agreement with the base contracting office to outline specific responsibilities that will ensure security requirements are incorporated into all base contracts.

1.6.5.2. Integrate on-base contractor operations into the installation Information Security Program in accordance with AFPD 31-6, para 7 and this instruction.

1.6.5.3. Review pre-award and/or draft solicitations, contract documents, security classification guides, and DD Form 254 to ensure appropriate security clauses and/or language is contained therein which address the protection of government information and sensitive resources.

1.6.5.4. Serve as technical OPR for the development and preparation of the VGSA or other security agreements as determined necessary by the IC.

1.6.5.5. Maintain a folder on each on-base contractor for which a VGSA has been executed.

1.6.5.6. Conduct security oversight of an on-base designated "cleared facility" as determined by the IC. A cleared facility operates under the security guidance of the NISPOM, installation security program guidance or a combination thereof.

1.6.5.7. Ensure the contractor takes prompt corrective actions when security program deficiencies are identified and promptly report security violations and/or compromises.

1.6.5.8. Forward to DSS a copy of the security review and survey reports and other applicable documentation, which pertains to an on-base "cleared facility" per DOD 5220.22-M, DOD 5220.22-R, AFPD 31-6, and this instruction, if required.

1.6.5.9. Participate and/or provide input during the source selection process, incentive awards evaluation process, etc.

## **1.7. Public Release of Information.**

**1.7. (AETC)** At least 6 months before hosting any meeting requiring foreign participation, send requests for foreign release through the command foreign disclosure officer, Air Force Security Assistance Training Squadron (AFSAT/CCD).

1.7.1. Contracting offices (COs) forward contractor's requests for public release of information relating to Air Force classified contracts or programs to the installation Public Affairs (PA) office. The PA office processes the request in accordance with AFI 35-101, *Public Affairs Policies and Procedures*, Chapter 15, Security and Policy Review and Chapter 18, News Media and Public Affairs.

1.7.1.1. Information requiring Air Force or DOD-level review will be forwarded by the entry-level public affairs office to the Secretary of the Air Force (SAF) Office of Public Affairs (SAF/PAS), 1690 Air Force Pentagon, Washington DC 20330-1690. SAF/PAS forwards the requests, as required, to the Directorate for Freedom of Information and Security Review (DFO-SIR), Washington Headquarters Service, Department of Defense, Pentagon, Washington DC 20301-1400.

1.7.2. When a contractor reports that classified information has appeared publicly, follow the guidelines in these documents: DOD 5200.1-R, *Information Security Program Regulation*; Air Force Policy Directive (AFPD) 31-4, *Information Security*; and Air Force Instruction (AFI) 31-401, *Information Security Program Management*.

## **1.8. Reporting Requirements.**

### **1.8.1. Reporting Adverse Information and Suspicious Contact Reporting.**

1.8.1.1. On-base integrated visitor groups satisfy NISPOM adverse information and suspicious contacts reporting requirements by notifying or submitting the appropriate report or information to the ISPM through the AF activity they support. This reporting provision must be outlined in the visitor group security agreement (VGSA), when applicable. On-base designated “cleared facilities” make reports or submit information directly to the ISPM.

1.8.1.2. Upon receipt of information submitted per paragraph **1.8.1.**, the ISPM will forward the report to the visitor group’s Home Office Facility (HOF). Any subsequent or additional reporting required by the NISPOM to other federal agencies, e.g., CSA, CSO, Federal Bureau of Investigations (FBI), is thereafter the responsibility of the HOF.

1.8.1.3. The ISPM will retain a copy of the adverse information or suspicious contact report in the visitor group’s files for 2 years.

1.8.1.4. The ISPM is responsible for notifying other AF activities, e.g., contracting office, Air Force Office of Special Investigations (AFOSI), when appropriate.

### **1.8.2. Reporting Security Violations.**

1.8.2.1. A designated on-base “cleared facility” reports the loss, compromise, suspected compromise or other security violations pursuant to the NISPOM through the ISPM, who in-turn is responsible for notifying the CSO.

1.8.2.2. On-base integrated visitor groups report such incidents and/or information in accordance with AFI 31-401 to the ISPM via the AF activity security manager. This reporting requirement must be specified in the VGSA, if applicable. The commander of the AF activity being supported appoints an assigned federal employee (military or civilian) to conduct the preliminary inquiry in accordance with AFI 31-401, Chapter 9.

1.8.2.3. The CSO and ISPM report significant contractor security violations and compromises (resulting in actual loss or compromise) of classified information to the contracting officer.

### **1.8.3. Reporting Espionage, Sabotage, and Subversive Activities.**

1.8.3.1. The ISPM reports 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 Air Force installations to the servicing AFOSI. AFOSI coordinates

with the FBI, as appropriate. The ISPM sends a report via secure communications (STU III or classified fax) with an information copy to each of the following activities:

1.8.3.1.1. Cognizant Security Office (CSO)

1.8.3.1.2. Functional Office of Primary Responsibility (OPR)

1.8.3.1.3. Headquarters United States Air Force, Information Security Division (HQ AF/XOFI)

1.8.3.1.4. Headquarters United States Air Force, Public Affairs (SAF/PA)

1.8.3.1.5. Appropriate Major Command (MAJCOM) Headquarters

1.8.3.2. Such a report should:

1.8.3.2.1. Identify the cleared facility or integrated visitor group involved.

1.8.3.2.2. Identify the contractor involved. Identify the person(s) involved, including the full name, date and place of birth, social security number, local address, present location, position with the contractor, security clearance (including past or present participation in any special access programs (SAPs), and a description of any plans or action and any recommendations to suspend or revoke the individual's personnel security clearance (PCL).

1.8.3.2.3. Establish the known circumstances of the incident, including the identity of the classified material involved; any subsequent activities or circumstances (including whether and which news media know about the incident); and culpable individuals, where known.

1.8.3.2.4. Document when (time and date) the ISPM reported the incident to the AFOSI or when the CSO reported the incident to the FBI, if known.

1.8.3.2.5. Include a copy of any investigative reports.

1.8.3.2.6. Identify any changes in contractor procedures necessitated by the incident and any recommendations for change in the security program, which might prevent similar future violations.

1.8.4. The reporting requirement outlined in paragraph **1.8.3.** is exempt from licensing with a report control symbol (RCS) IAW paragraph 2.11.1. of AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public and Interagency Air Force Information Collections.*

1.8.5. Reporting Loss, Compromise, and Possible Compromise.

1.8.5.1. ICs follow this instruction and perform actions as directed by DOD 5220.22-R, *Industrial Security Regulation*, to report the loss, compromise, or possible compromise of classified information for on-base contractor operations for which the Air Force has retained security oversight.

1.8.5.2. Contracting officers who learn of contractor loss, compromise, or possible compromise of classified information immediately notify the servicing ISPM and the Air Force functional office that has responsibility for the compromised information.

1.8.5.3. The original classification authority (OCA) or designated organization is responsible for determining whether a damage assessment is warranted and making any subsequent

1.8.5.4. The OCA or designated organization notifies the Air Force activity, CSO, and/or the contractor of decisions to declassify, downgrade, or retain classification of the affected information. Do not give copies of damage assessment reports to the CSO or contractor operation.

1.8.5.5. Unless assistance is needed, do not notify the CSO of action begin taken to mitigate damage to national security.

1.8.5.6. Correspondence associated with or related to any such incidents should be handled between the CSO and/or ISPM and the affected Air Force activity direct.

1.8.5.7. The ISPM provides copies of investigation and inquiry reports to the appropriate CSO and HOF that has jurisdiction over the contractor operation.

## Chapter 2

### SECURITY CLEARANCES

#### 2.1. Facility Security Clearances (FCLs).

2.1.1. Sponsoring FCLs. The contracting office (CO) is responsible for Facility Security Clearance (FCL) sponsorship. Defense Security Service - Operating Center Columbus (DSS-OCC) is the authorizing agent for the FCL. DSS-OCC establishes and maintains all FCLs within the NISP. Also see DOD 5220.22-M, DOD 5200.2-R, *Personnel Security Program*, AFD 31-5, *Personnel Security*, and AFI 31-501, *Personnel Security Program Management*.

2.1.1.1. To request an FCL sponsorship, write to the CSO with oversight responsibility for the sponsored facility.

2.1.1.2. Give the full name for the sponsored facility, its physical and mailing address, telephone number, and a specific point of contact at the facility, when known. Give the full name, job title, and direct-dial telephone number of the Air Force sponsor.

2.1.1.3. Establishing final FCLs through DSS-OCC may take several months. When circumstances do not permit such delays, sponsors may request an interim FCL through OCC.

2.1.2. Sponsoring Interim FCLs. DSS-OCC automatically processes all requests for Confidential and Secret FCLs for interim clearances when possible. However, Air Force sponsorship of interim Top Secret FCLs must be justified on a case-specific basis in accordance with DOD 5220.22-R. To request a Top Secret interim FCL, the CO prepares and routes sponsorships through command channels to the MAJCOM, FOA, or DRU commander for approval. Each request must include these items:

2.1.2.1. An explanation of why an interim Top Secret FCL would prevent a crucial delay in the award or performance of a classified contract.

2.1.2.2. A listing giving the legal name of the facility being sponsored, its complete street address, and the names and positions of people who are applying for interim Top Secret access authorization.

2.1.2.3. The address of the authorizing DSS.

2.1.3. Establishing FCLs. DSS-OCC establishes and maintains FCL for contractor operations participating in the NISP.

2.1.3.1. The ISPM with oversight responsibility for a cleared facility conducts required security reviews of the operation and assists the CSO, as necessary.

2.1.3.2. The ISPM also conducts surveys and/or administrative inquiries pertaining to an on-base cleared facility as requested by the CSO and ensures contractor compliance with DOD 5220.22-M, NISPOM.

2.1.3.3. Complete the survey by using the DD Form 374, **Facility Security Clearance Survey Data Sheet**, [DOD 5220.22-R], or an equivalent/acceptable automated format when conducting survey for an on-base cleared facility and forward a copy to the CSO.

#### 2.2. Contractors with Foreign Ownership, Control or Influence (FOCI).

2.2.1. The CSO tells COs if a contractor performing on a classified contract has foreign ownership, control, or influence (FOCI) or whether it can be negated. Such influence might jeopardize the security of classified information held by the contractor.

2.2.2. To resolve a FOCI problem, the CSO may establish a facility clearance that limits the level and type of classified information to which a FOCI contractor has access. Such restrictions might affect ongoing, pending and future classified contracts with the contractor. The CO should discuss this impact with the ISPM and servicing Foreign Disclosure office.

2.2.3. The CO considers sponsoring a National Interest Determination (NID) after receiving written justification from the requesting program office or activity. This justification must address and explain how the FOCI contractor's product or service is crucial or is the sole available source to the AF. If applicable, the program or activity must also provide a written explanation when contract cancellation would cause unacceptable delays for mission-essential weapons systems in the field or for support organizations.

2.2.3.1. The requesting program office or activity is responsible for obtaining written release approval authority from the functional owner of the "proscribed information," prior to submitting the NID to the contracting office. The program office or activity contacts the OCA for Top Secret (TS), NSA for Communications Security (COMSEC), DCI for Sensitive Compartmented Information (SCI), and DOE for Restricted Data (RD) or Formerly Restricted Data (FRD) to obtain release approval. (NOTE: All release determination request (NID) involving/for SCI must be submitted to HQ USAF/XOIIS for review, coordination and processing).

2.2.3.2. The CO reviews, validates, and processes the NID and associated written approvals as follows:

2.2.3.2.1. Forward request for NID related to special access program (SAP) performance through the appropriate SAP and command channels to the Deputy for Security and Investigative Programs, Office of the Administrative Assistant (SAF/AAZ), 1720 Air Force Pentagon, Washington, D.C. 20330-1720 for approval.

2.2.3.2.2. Forward request for non-SAP NID through command ISPM channels to HQ USAF/XOFI for review and coordination. The NIDs are then be forwarded to SAF/AAZ for review and endorsement.

2.2.3.3. SAF/AA endorse the NID and forward it to the Director, Defense Security Programs, Office of the Deputy Assistant Secretary of Defense for Counterintelligence and Security Countermeasures, Office of the Assistant Secretary of Defense for Command, Control, Communication, and Intelligence (OASD/C3I), Pentagon, Washington, D.C. 20301-3040, for final approval.

### **2.3. Contractor Personnel Security Clearances (PCLs).**

2.3.1. Defense Security Service - Operating Center Columbus (DSS-OCC), formerly known as Defense Investigative Service (DIS) - Central Verification Activity (CVA), Personnel Investigative Center, an operational element of DSS, grants and maintains contractor PCLs. DSS-OCC also terminates contractor PCLs when the contractor no longer needs them or when a contractor employee terminates. Administrative termination of a PCL carries no adverse implications regarding the employee or the contractor.

2.3.2. The Directorate for Industrial Security Clearance Review, DOD Office of General Counsel, may suspend or revoke contractor PCLs following due process.

2.3.3. DSS automatically processes all requests for Confidential or Secret PCLs for interim clearances, where possible.

2.3.4. When a contractor employee who is not cleared for access to Top Secret information needs such access to perform on an Air Force classified contract, the employing contractor may sponsor the individual for an interim Top Secret PCL.

2.3.4.1. The contractor should send requests to the CO who seeks concurrence of the system program office (SPO), system manager (SM), or program manager (PM).

2.3.4.2. The contractor's request should document clearly why the individual needs an interim PCL, why contract requirements may not be satisfied with another individual more suitably cleared, and what the potential adverse impact would be on contract performance if an interim PCL were not granted. The contracting officer will deny contractor requests that do not meet these criteria.

2.3.4.3. The CO routes the appropriate contractor's request for interim Top Secret PCLs to the MAJCOM, FOA, or DRU commander for approval.

2.3.4.4. The CO sends favorably endorsed requests to the contractor, who then includes the endorsement in the personnel security questionnaire package for transmission to DSS-OCC for action. The CO promptly returns denied requests.

#### **2.4. Processing Trustworthiness Determinations.**

2.4.1. When contractors require *unescorted entry to restricted areas, access to sensitive unclassified information, access to government automated information systems (AIS) and/ or sensitive equipment*, not involving access to classified information, the contractor's personnel security questionnaire is processed by the sponsoring Air Force activity per DOD 5200.2-R and AFI 31-501.

**2.5. Reciprocity.** The CO, ISPM, and other installation security disciplines offices of primary responsibility (OPRs) work together to resolve issues pertaining to reciprocity, as applicable to inspections, surveys, audits, security clearances, security reviews, etc. Elevate reciprocity issues to the next higher level of command when they can not be resolved locally.

## Chapter 3

### SECURITY TRAINING AND BRIEFINGS

#### 3.1. Security Training Requirements.

3.1.1. Air Force classified solicitations and/or contracts [Statement of Objectives (SOO), Statement of Work (SOW), Request for Bid (RFB), Request for Quote (RFQ), VGSA, etc.] may stipulate contractor compliance with and participation in pertinent Air Force, command and installation security training programs when performance or services will occur on an Air Force installation.

3.1.2. When specified in an executed VGSA, AFI 31-401, *Information Security Program Management*, security training requirements satisfy the NISPOM training provision for on-base integrated visitor groups. Other Air Force functionals and/or security discipline OPRs may use this training provision for operational efficiency, however the specific requirements must be identified in the VGSA.

3.1.3. When an on-base contractor operation is designated as a cleared facility, the ISPM will provide the initial facility security officer (FSO) briefing in accordance with the NISPOM and CSO guidance.

3.1.4. Air Force unit security managers or security officers will provide information security program training (initial, refresher and annual) and other security awareness support to integrated visitor groups. The AF activity, working in concert with the ISPM, will incorporate language into the VGSA, which requires visitor group personnel to attend and/or receive information security training per DOD 5200.1-R and AFI 31-401, Chapter 8. Unit security managers will ensure integrated visitor group personnel are included in their security education program.

**3.1.4. (AETC)** Contractors will complete all training requirements prior to being granted access to the base computer network.

#### 3.2. Security Briefing/Debriefing Requirements.

3.2.1. Management officials of the on-base cleared facility visitor groups are responsible for ensuring their employees receive all required security briefings and debriefings as mandated by the NISPOM.

3.2.2. For integrated visitor groups, DOD 5200.1-R and AFI 31-401 security training requirements are equivalent to and satisfy the training requirements of NISPOM, where appropriate. On-base contractor management officials are responsible for ensuring their personnel's attendance and satisfying NISPOM documentation requirements.

3.2.3. The ISPM will invite on-base cleared facility, Facility Security Officers (FSOs) and/or security representatives, to the installation's information security manager meetings.

**3.2.3. (AETC)** The FAC and the ISPM will determine the extent of visitor group security management responsibilities, as reflected in the VGSA. The VGSA will require contractor visitor groups to implement DoD 5200.1-R and AFI 31-401. The contractor security manager will attend semiannual security manager meetings hosted by the ISPM. The ISPM will forward announcements of these meetings to the FAC and the contractor security manager.

## Chapter 4

### SECURITY SPECIFICATIONS AND GUIDANCE

#### 4.1. Issuing Security Classification Guidance.

4.1.1. The AF program, project, activity and contracting office (CO) implements NISPOM, DOD 5200.1-R, and installation security requirements through contract documents. Only COs can sign, modify or negotiate changes to contracts.

4.1.2. When a contractor requires access to classified information, the AF program, project or activity prepares the required DD Forms 254, **DOD Contract Security Classification Specifications**. The contractor should use the security requirements in this form to accurately estimate the cost of security measures. More detailed security requirements are specified in the statement of work (SOW), statement of objectives (SOO), performance work statement (PWS), Visitor Group Security Agreement (VGSA), etc.

**4.1.2. (AETC)** The ISPM will use SOW and PWS security templates established by HQ AETC/SFI. These templates, located on the HQ AETC/SF web page (<https://www.aetc.af.mil/sf/>) under the Information Security Division, Industrial Security Branch, will be used for both classified and unclassified base contracts.

4.1.3. The responsible AF program, project, or activity will identify (by title, functional OPR, and approval date), the specific security classification guidance or guides (SCGs) applicable to the contract in Block #13 of the DD Form 254. The AF activity/program will provide copies of the SCG to the contractor prior to the contract commencing.

#### 4.2. DD Form 254, Contract Security Classification Specifications.

4.2.1. The AF program, project or activity prepares an *initial* draft DD Form 254 for each classified contract. When drafting the *initial* DD Form 254s, the program, project or activity will consult with the CO, ISPM, and other installation security discipline or functional OPRs affected under the terms of the solicitation/contract to ensure accuracy. Once drafted, the *initial* draft of the DD Form 254 is forwarded to the CO for processing.

4.2.2. The CO reviews and coordinates the *initial* draft DD Form 254 with all affected security disciplines and functionals, as appropriate. This action ensures that approved security guidance is being provided to the contractor. Once the *initial* review has been completed, the requesting AF entity/activity incorporates the necessary changes and forwards the *final* DD Form 254 to the CO for subsequent approval and signing.

4.2.3. Prior to signing the *final* DD Form 254, the CO will coordinate the form with the affected security disciplines and/or functional OPRs. This review and coordination must be indicated in Block 13 (office symbol, date and initials of reviewer) of the *final* DD form 254. When SAPs are involved, coordinate draft DD Form 254 with the office responsible for SAP security oversight. Keep DD Forms 254 for SAPs unclassified when possible.

#### 4.3. Reviewing and Certifying the DD Form 254.

4.3.1. The ISPM reviews the *initial* draft and *final* DD Form 254 to ensure that the security classification guidance is accurate, approved, and appropriate. Other security requirements are incorporated into the SOW, SOO, PWS, VGSA, etc.

4.3.2. The AF program, project, or activity reviews the DD Form 254 and applicable security classification guides (SCGs) every two years to ensure accuracy and currency. When changes are necessary, the contract will be modified, if appropriate and revised guidance issued.

**4.3.2. (AETC)** After guidance has been reviewed, the FAC will notify agencies that received the original DD Form 254. He or she will make the notifications in writing and identify the (1) contractor, (2) agency using the contractor service, (3) commercial and government entity (CAGE) code (DD Form 254, Item 6b), and (4) clearance level (DD Form 254, Item 1a). The FAC will annotate the next required review date on the notification memorandum, attach it to the DD Form 254, and prepare a revised DD Form 254 when changes are required. **NOTE:** In AETC, the FAC, along with the program and project managers, monitors and conducts required classification reviews.

4.3.3. The CO certifies (signs) the DD Form 254, Block 16e. At the CO discretion, this authority may be delegated (in writing) as authorized by the Federal Acquisition Regulations (FAR) or supplementation thereto.

#### **4.4. Distribution of the DD Form 254.**

4.4.1. When DSS is relieved of security oversight responsibility for cleared facilities performing on SCI or SAP programs, furnish Headquarters DSS, 1340 Braddock Place, Alexandria VA 22314-1651, a copy of the DD Form 254.

4.4.2. When a contractor's performance will be on Air Force installation, the AF program, project or activity must identify/specify all contract performance locations, if known, on the DD Form 254. When the contract is performed elsewhere, the CO will provide a copy of the signed DD Form 254 to that location's ISPM.

**4.4.2. (AETC)** HQ AETC and base-level PCOs will send HQ AETC/SFI a signed copy of all DD Forms 254, ensuring HQ AETC/SFI is listed in Item 17.

4.4.3. Procuring Contracting Officers (PCOs), their designated representatives, including Administrative Contracting Officers (ACOs), distribute DD Form 254.

#### **4.5. Visitor Group Security Agreement (VGSA).**

4.5.1. Execute a VGSA with all contractor operations located on Air Force installations that will require access to classified information. At the IC's discretion, the VGSA execution requirement may be extended to contractors performing on contracts that require access to sensitive unclassified information, sensitive resources or frequent "entry" to the installation.

4.5.2. The installation ISPM, security disciplines and functional OPRs work in concert with the AF program, project and/or activity to develop the Visitor Group Security Agreement (VGSA) requirements. The requirement to execute a VGSA is in addition to preparing the DD Form 254.

4.5.3. The VGSA must address those security requirements and/or procedures that are unique to the *installation* for which the contractor will be held contractually liable. VGSA's need only address those areas of security, safeguarding and/or protection that have not been covered elsewhere within the contract, DD Form 254, SOW, SOO, PWS, etc.

4.5.4. The ISPM is the technical OPR for development and preparation of the VGSA. For coordination purposes, the ISPM routes the VGSA to all *installation* security discipline OPRs and/or other agencies lending expertise to the contractual security requirements.

4.5.5. The ISPM signs the VGSA on behalf of the installation commander. The ISPM forwards a copy of the executed/signed VGSA to the contracting officer who awarded the contract or to the contracting officer's designated representative, when appropriate.

**4.5.5. (AETC)** The FAC will sign the VGSA to ensure the sponsoring agency is in agreement with the security requirements.

4.5.6. An authorized company official shall sign the VGSA. The CO will file a copy of the authorization with the contract.

## Chapter 5

### SAFEGUARDING

**5.1. Designation of On-Base Visitor Groups.** The IC works in concert with the Air Force activity, CO and ISPM to determine the designation of an on-base visitor group (cleared facility, integrated visitor group or intermittent visitor).

#### **5.2. Integrated Visitor Group.**

5.2.1. Integrated visitor groups operate in accordance with DOD 5200.1-R and supplemental guidance thereto. They handle, generate, process, and store classified information per AF guidance. The exception being, their “access” is limited to “need-to-know” contract-specific classified performance information.

5.2.2. The AF must stipulate the specific DOD 5200.1-R and supplemental guidance, which is applicable under the terms of the executed VGSA.

5.2.3. The guidance conveyed to on-base contractor operation via the VGSA is limited to the AF installation and the AF solicitation/contract which it was executed to support. All other NISPOM mandated security requirements not addressed or specifically exempted by the executed VGSA or other contracting document must be implemented by the contractor.

5.2.4. The VGSA must clearly reflect that the Air Force is accountable for and controls all classified information. Integrated contractor visitor groups are prohibited from establishing separate classified information controls. (NOTE: Integrated visitor group personnel *can not* be appointed as primary or alternate security managers for AF activities. However, they can be required (via the VGSA) to provide other security program support, under AF direction, such as, conducting end-of-day security checks, security training/briefings, etc.).

**5.3. Cleared Facility.** A cleared facility operates under the mandates of the NISPOM and/or installation security program requirements or a combination thereof. See AAFP 31-6 for further guidance regarding their establishment.

**5.4. Intermittent Visitors.** Intermittent visitors may operate under the security requirements of the NISPOM or the installation security program. The IC makes this determination after considering the intermittent visitor’s relationship and interface with the AF activity and/or installation.

**5.5. On-Base Contract Completion or Termination.** The program, project or AF activity will notify the ISPM in writing when the contractual services and/or performance has been completed or terminated.

## Chapter 6

### OVERSIGHT REVIEWS AND REPORTING REQUIREMENTS

#### 6.1. Conducting Industrial Security Reviews (SRs).

6.1.1. Industrial Security Reviews. The ISPM conduct security reviews (SRs) of on-base cleared facilities that performs classified work on Air Force installations. Such SRs evaluate the contractor's compliance with contract specific-security requirements and pertinent DOD and Air Force security instructions.

6.1.2. Scheduling Industrial Security Reviews. Conduct (SRs) of on-base cleared facilities per DOD 5220.22-M and DOD 5220.22-R. Unless conducting an unannounced security review on a cleared facility, provide contractor activity's management 30 days advanced written notification.

6.1.3. Performing Industrial Security Reviews. ISPMs coordinate with other Air Force security discipline OPRs such as; Operations Security (OPSEC), Computer Security (COMPUSEC) and Communications Security (COMSEC), to provide specialized expertise when necessary to complete a security review. The SR is complete when all security requirements imposed under the terms of the contract have been evaluated.

6.1.3.1. When SRs are conducted for cleared facilities, provide copies of completed SR report, with all related correspondence, to the CSO. Use DSS' automated format to document the results of the SR. Contact HQ USAF/XOFI to obtain a copy of the automated DSS format.

6.1.3.2. Facility security clearance (FCL) files must contain all key documentation prescribed by DOD 5220.22-R and the CSO, to include DD Form 254 and related contract security requirement documents.

#### 6.1.4. Post-Industrial Security Review Requirements.

6.1.4.1. Send a letter/report to senior management officials of the cleared facility within 10 days of completing the security review. The letter should:

6.1.4.2. Confirm the contractor's security status as discussed during the exit interview.

6.1.4.3. List any deficiencies requiring corrective action.

6.1.4.4. Within 30 days, request written confirmation on the status of any open major discrepancy (condition which resulted in or could reasonably be expected to result in the loss or compromise of classified information).

6.1.4.5. The ISPM may extend the time for corrective action if required changes are significant and the contractor is making a conscientious effort to resolve problems expeditiously.

#### 6.1.5. Unsatisfactory Industrial Security Reviews.

6.1.5.1. The ISPM assigns an on-base cleared facility an unsatisfactory SR rating:

6.1.5.1.1. To a cleared facility visitor groups if it fails to satisfactorily perform its contractual security responsibilities.

6.1.5.1.2. When major failures in the contractor's security program have resulted in or could reasonably be expected to result in the loss or compromise of classified information.

6.1.5.1.3. When the contractor is clearly responsible for the security problems cited during a security review.

6.1.5.1.4. The ISPM coordinates with the CSO and contracting officer when assigning an unsatisfactory SR rating for an on-base cleared facility.

6.1.5.1.5. The home office facility (HOF) for the cleared facility is ultimately responsible for meeting contract security requirements. When assigning an unsatisfactory SR rating, the ISPM notifies the HOF immediately through the contracting office and requests prompt and complete corrective action. If the HOF fails to take corrective action, its security clearance may be affected. The servicing security activity should notify the HOF's CSO if problems continue.

#### 6.1.6. Invalidating the Facility Security Clearance (FCL).

6.1.6.1. The CSO notifies the contracting officers in writing when the FCL of a contractor under their jurisdiction is invalidated.

6.1.6.2. A contractor who fails to correct security deficiencies that subsequently results in invalidation may lose its FCL.

6.1.6.3. Although most contractors resolve invalidations promptly, contractors with foreign owned, controlled, or influence (FOCI) invalidations may have to wait for many months. Where FOCI is evident, the facility clearance may remain invalidated for more than a year while methods to resolve the FOCI are considered, approved, and implemented. The FCL is invalidated while DSS negotiates voting trusts, proxy agreements, or special agreements with foreign interests.

6.1.6.4. Document SR for an on-base cleared facility as required by the DOD 5220.22-M, DOD 5220.22-R, and CSO guidance. Keep copies of completed SR reports with pre-security review letter and completed post-review correspondence for 2 years from the date of the most recent SR.

6.1.6.5. Maintain copies of self-inspection reports or reviews for 2 years from date of the most recent self-inspection.

## 6.2. Conducting Information Security Program Reviews.

6.2.1. Information Security Program Reviews. On-base integrated visitor groups will be evaluated and conduct self-inspections collectively with the AF activity per DOD 5200.1-R and AFI 31-401, guidance. Integrated visitor groups will not be subjected to the SR requirements of the NISPOM. The installation prescribes the report for documenting program reviews.

**6.2.1. (AETC) DD Form 696, Industrial Security Inspection Report**, will not be used to document results of industrial security inspections for onbase integrated visitor groups. Instead, annual program review and semiannual self-inspection reports will be used to record the contractor's security compliance. Unit security managers will ensure onbase visitor groups are included in the semiannual self-inspection program. The unit security manager will provide the FAC, contractor security manager, and ISPM with a copy of the results of the semiannual self-inspections. The unit security manager will ensure a semiannual self-inspection is conducted on contractor visitor groups. (A government representative must conduct the self-inspection.)

6.2.2. Scheduling Information Security Program Reviews. Schedule program reviews per DOD 5200.1-R and AFI 31-401 guidance.

6.2.3. The AF activity is responsible for ensuring its integrated visitor group implement and comply with DOD 5200.1-R and AFI 31-401 requirements.

**6.2.3. (AETC)** All Air Force visitor groups, regardless of their level of access, will receive an initial program review within 30 days after the contract start date. After this initial program review, visitor groups will be checked as part of the sponsoring activity's semiannual self-inspection program. The ISPM is responsible for conducting program reviews annually. The quality assurance evaluator or FAC will be involved with semiannual self-inspections and program reviews.

6.2.4. The ISPM, unit security manager and integrated visitor group establishes files and maintain the following documentation, as appropriate:

6.2.4.1. Signed copy of the DD Form 254 and any revisions.

6.2.4.2. Signed copy of the VGSA. (**NOTE:** Maintaining a copy of the VGSA is *optional* for the ISPM).

6.2.4.3. Current listing of the key on-base management officials or representatives.

6.2.4.4. Copy of the last annual program review.

6.2.4.5. Copies of last two self-inspections reports. The annual program review can be used to substitute for one of the self-inspections. (**NOTE:** The maintenance of self-inspection reports is optional for ISPMs).

6.2.4.6. Copy of contractor's visit authorization letter (VAL). (**NOTE:** In addition, the unit security manager will maintain a copy of each outgoing/incoming VAL generated by or directed to the integrated visitor group).

6.2.5. For visitor groups, the ISPM briefs key Air Force and designated visitor group managers on the status of the unit's security program. Provide both parties a copy of the PR report and any other related assessment, survey or staff assistance visit (SAV) report. Do not furnish copies of these reports to the CSO.

6.2.5.1. When warranted, AF commanders notify the contractor's home office facility (HOF), in writing, through the contracting office of major security program deficiencies or non-compliance with the terms of the VGSA.

6.2.6. The ISPM will maintain files/records on each on-base integrated visitor group in accordance with paragraph **6.2.4.**, this publication.

## Chapter 7

### VISITS AND MEETINGS

**7.1. Installation Visitors.** The installation commander is the sole authority responsible for granting contractors access to the installation, regardless of which DOD agency, military service component, or activity awarded the contract.

**7.1. (AETC)** When sponsoring (or cosponsoring) and/or conducting meetings about DoD-related scientific papers, follow the guidance in AFI 61-205, *Sponsoring or Co-Sponsoring, Conducting, and Presenting DoD-Related Scientific Papers at Unclassified and Classified Conferences, Symposia, and Other Similar Meetings*.

**7.2. Visitor Groups.** The IC designates contractors who require access to the installation in the performance of a government contract as intermittent visitors, integrated visitor groups, or cleared facilities.

#### **7.3. Contractor Visits to Air Force Installations.**

7.3.1. DOD contractors located on or visiting Air Force installations in support of a classified contract must comply with DOD 5220.22-M, Chapter 6, Section 1, visit requirements.

7.3.2. Installation commanders establish procedures for processing and coordinating incoming contractor visit requests. For integrated visitor groups, the AF activity is the authorizing/approval authority for incoming and outgoing visit authorization letters (VALs) or similar request. The AF activity is responsible for publishing on-base VAL processing procedures.

**7.3.2. (AETC)** Contractors performing duties normally performed by military or DoD civilian personnel fit the category of integrated visitor groups. (Examples include supply, information management, audiovisual and reprographics services, and aircraft maintenance.) The contracting office will tell contractors to address visit request letters to the sponsoring unit or agency.

7.3.3. Identify specific procedures for receiving, processing, and handling incoming visitor group visit request in the VGSA and AF activity's information security program operating instruction (OI). Whenever possible, these incoming request should be directed to and maintained on file by the AF activity's unit security manager.

**7.4. Air Force Visits to Contractor Facilities.** Air Force personnel who require access to classified information while visiting contractor facilities must comply with the provisions of DOD 5200.1-R and DOD 5220.22-M.

## Chapter 8

### SUBCONTRACTING

#### 8.1. Prime Contractor's Responsibilities.

8.1.1. Prime contractors are responsible for ensuring their on-base subcontractors are knowledgeable of and comply with the applicable security requirements (NISPOM, installation, etc.) as identified in contracts and/or other contracting documents.

8.1.2. Prime contractors supporting classified efforts must include a provision in each on-base sub-contract that requires subcontractors to contact the installation commander or designee and execute a VGSA prior to beginning on-base operations.

**8.2. Subcontractor Responsibilities.** On-base subcontractors must execute a separate and/or independent VGSA with the installation. (NOTE: As an alternative, when multiple subcontractor perform services in support of the same on-base classified contract and prime contractor, the execution of this VGSA, can be satisfied by the subcontractor acknowledging review and understanding of the security requirements identified in the prime contractor's executed VGSA. This being the case, executing and adding a signatory page *only* (attachment) to the prime's VGSA is acceptable).

## Chapter 9

### AUTOMATED INFORMATION SYSTEM (AIS) SECURITY

#### 9.1. Automated Information Systems (AIS) Accreditation.

9.1.1. When industrial security program oversight is retained by the Air Force for on-base cleared facilities, the CO coordinates automated information system (AIS) accreditation, Communications Security (COMSEC), and Emission Security (EMSEC) requirements with the responsible installation security discipline OPR, the ISPM and DSS, if appropriate.

**9.1.1.1. (Added-AETC)** (AETC) Communications security (COMSEC) information or material will not be released to contractors without approval of the command COMSEC manager (Network Operations and Security Flight [AETC CSS/SCNS]). When a contractor requires access or stores COMSEC material or documents, he or she will contact AETC CSS/SCNS for assistance.

**9.1.1.2. (Added-AETC)** (AETC) HQ AETC and wing COMSEC managers have functional responsibility for COMSEC materials and assessments as follows:

**9.1.1.2.1. (AETC)** AETC CSS/SCNS will provide the required COMSEC briefing for contractors to the contractor's primary and alternate COMSEC managers for onbase visitor groups overseen by the ISPM at those locations where the contractor is responsible for a COMSEC account. The wing COMSEC manager will provide the briefing when the contractor will be a COMSEC user off the wing account. In all cases, these briefings will be documented and re-accomplished on an annual basis.

**9.1.1.2.2. (AETC)** AETC CSS/SCNS will conduct command COMSEC assessments of all contractor-operated COMSEC accounts and contractors who store COMSEC documents that are obtained from the wing COMSEC account. AETC wing COMSEC managers will conduct assessments of all contractors holding COMSEC material.

**9.1.1.3. (Added-AETC)** (AETC) Applicable emission security (EMSEC) clauses will be referenced in DD Form 254, Item 11i. The DD Form 254 will be coordinated with the local wing EMSEC manager before obtaining ISPM coordination.

9.1.2. Integrated visitor groups use approved Air Force AISs and/or networks to process classified and sensitive unclassified information.

**9.1.2. (AETC)** The contract document will outline contractor responsibilities for protection of government sensitive unclassified information in contractor automated information system (AIS) equipment.

**9.1.2.1. (Added-AETC)** (AETC) COMPUSEC procedures are as follows:

**9.1.2.1.1. (AETC)** Integrated visitor group contractors will participate in the wing-level COMPUSEC program to ensure all AISs meet standards for the protection of Air Force information.

**9.1.2.1.2. (AETC)** All contractor-owned, contractor-operated AISs that process Air Force information must meet the applicable criteria contained in AFI 33-202, *Computer Security*, Chapter 3.

**9.1.2.1.3. (AETC)** The chief of the information assurance (IA) office will provide the ISPM with a courtesy copy of all annual staff assistance visits to the contractor.

**9.1.2.2. (Added-AETC)** (AETC) EMSEC procedures are as follows:

**9.1.2.2.1. (AETC)** Contractors will participate in the wing-level EMSEC program, where applicable. Equipment used by contractors for the processing of classified information must be assessed and approved, in writing, by the wing EMSEC manager.

**9.1.2.2.2. (AETC)** Contractors must follow EMSEC countermeasures established by the wing EMSEC manager.

**9.1.2.2.3. (AETC)** The wing EMSEC manager will send the ISPM a copy of the approval authority for equipment used by contractors for processing classified Air Force information. He or she will also send the ISPM a copy of annual visits to contractor integrated visitor groups and cleared facilities.

9.1.3. Contractor employees who require access to government AISs under the terms of a government contract must be determined to be “trustworthy” by a designated government official prior to AIS access being granted. Process all contractors AIS access personnel security investigation (PSI) in accordance with DOD 5200.2-R and AFI 31-501. This requirement must be specified in the basic solicitation and/or contract documents.

9.1.4. Contracts or solicitations (classified and unclassified) involving the use, operation, maintenance, etc., of AIS will be routed through the installation Communications and Information (SC) activity for review and coordination.

**9.1.4. (AETC)** The applicable wing IA office will review and coordinate on DD Forms 254 where the contractor is required to hold or use COMSEC material or participate in wing-level COMPUSEC, EMSEC, and security awareness, training, and education (SATE) programs.

## Chapter 10

### SPECIAL REQUIREMENTS

**10.1. Special Access Program.** For a carve-out contract, the Special Access Program (SAP) program manager assigns an Air Force element to perform security reviews and oversight. (Also see DOD 5220.22M-Sup 1, National Industrial Security Program Operating Manual (NISPOM) Supplement, and AFI 16-701, Special Access Programs.)

**10.2. Sensitive Compartmented Information.** Program managers for Air Force SAP and SCI programs may relieve the designated CSO and servicing security activity from security review and oversight responsibility for cleared facilities and/or visitor groups. Such relief normally will be limited to specific SAP and SCI information.

**10.2. (AETC)** In HQ AETC, the SSO is responsible for (1) approving security attachments that outline contractor security requirements for SCI, (2) establishing SCI facilities, (3) granting SCI access, and (4) coordinating on any DD Form 254 (including requests for bid or proposal, original DD Forms 254 for awarded contracts, and revised and final DD Forms 254, if issued, that require SCI access). Each AETC base with an SSO will perform this function at the local level for contracts awarded for work at the base.

## Chapter 11

### INTERNATIONAL SECURITY REQUIREMENTS

**11.1. Procedures for Contractor Operations Overseas.** DOD policy does not allow an FCL to be issued for contractors located outside the US, Puerto Rico, or a United States possession or trust territory. Treat DOD contractor operations supporting the Air Force overseas as visitor groups.

**11.2. Disclosure of Information to Foreign Visitors/Interests.** Visits by foreigners to contractors performing on Air Force contracts (whether on or off base) that requires access to classified or controlled unclassified information will be processed through the Foreign Visits System IAW AFI 16-201. Approved visits will include disclosure authorization through the installation or servicing Air Force foreign disclosure office. Visits may be non-sponsored by the Air Force in which case the visit may take place but disclosure will be limited to information in the public domain or information covered by a valid export license issued by the Department of State IAW the Arms Export Control Act. Any disclosure of classified information must be on a government-to-government basis.

**11.3. Documentary Disclosure of Information to a Foreign Entity.** Contractors performing on Air Force contracts will submit request for documentary disclosure of classified or controlled unclassified information to the contracting officer. The contracting officer validates the need for disclosure and forwards the information to the installation or servicing foreign disclosure office which process the request IAW AFI 16-201

**11.4. Foreign Visits .** All visit requests submitted by or on behalf of a foreign visitor must be processed through the installation and/or MAJCOM foreign disclosure activity, at least 30 days in advance of the intended arrival date.

## Chapter 12

### OTHER APPLICABLE SECURITY GUIDANCE

**12.1. Security Plans, Procedures, Operating Instructions and Training Material.** Integrated visitor groups use existing Air Force security program related plans (Operations Security, Program Protection, Automated Information Systems, etc.), procedures, operating instructions (OIs), and educational/training materials that meet the intent of and satisfy NISPOM requirements. Coordinate with other security discipline OPRs, when applicable, and incorporate authority for their usage in the VGSA or other appropriate contracting documents.

**12.1. (AETC)** Base OPSEC program managers will provide guidance on OPSEC requirements and send contractor OPSEC plans to HQ AETC/DOYI for approval.

#### **12.2. Applicability of Other Security Program Requirements.**

12.2.1. Coordinate security requirements, not stipulated in the NISPOM, with the responsible security discipline OPR and DSS, if applicable.

12.2.2. Functional specialists representing related security programs may accompany the ISPM or CSO representative during security reviews or when requested.

**12.3. (Added-AETC) (AETC) Forms Adopted.** DD Forms 254 and 696.

JAMES M. SHAMESS, Brig General, USAF  
Director of Security Forces

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

Executive Order 12829, *National Industrial Security Program*, 7 Jan 93

Executive Order 12958, *Classified National Security Information*, 20 Apr 95

DOD 5200.1-R, *Information Security Program*

DOD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*

DOD 5220.22-M-Sup 1, *National Industrial Security Operating Manual Supplement (NISPOMSUP)*

DOD 5220.22-R, *Industrial Security Regulation*

AFPD 10-11, *Operations Security*

AFPD 31-4, *Information Security*

AFPD 31-5, *Personnel Security Program Policy*

AFPD 31-6, *Industrial Security*

AFI 31-401, *Information Security Program Management*

AFI 31-501, *Personnel Security Program Management*

AFI 31-601, *Industrial Security Program Management*

AFI 33-203, *Emission Security*

AFI 35-101 *Air Force Public Affairs Policies and Procedures*

AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public and Interagency Air Force Information Collections*

AFH 31-602, *Industrial Security Program*

***(Added-AETC) References***

Atomic Energy Act of 1954

Federal Acquisition Regulation (FAR)

AFI 33-202, *Computer Security*

AFI 61-205, *Sponsoring or Co-Sponsoring, Conducting, and Presenting DoD-Related Scientific Papers at Unclassified and Classified Conferences, Symposia, and Other Similar Meetings*

***(Added-AETC) Abbreviations and Acronyms***

**ACO**—Administrative Contracting Officer

**AFH**—Air Force Handbook

**AFI**—Air Force Instruction

**AFOSI**—Air Force Office of Special Investigations  
**AFPD**—Air Force Policy Directive  
**AIS**—Automated Information System  
**CO**—Contracting Office  
**COMSEC**—Communications Security (COMSEC)  
**CSO**—Cognizant Security Office  
**DSS-OCC**—Defense Security Service - Operating Center Columbus  
**DOD**—Department of Defense  
**DRU**—Direct Reporting Unit  
**DSS**—Defense Security Service  
**EMSEC**—Emanation Security  
**FAR**—Federal Acquisition Regulation  
**FBI**—Federal Bureau of Investigations  
**FCL**—Facility Security Clearance  
**FOA**—Field Operating Agency  
**FOCI**—Foreign Ownership, Controlled, or Influenced  
**HOF**—Home Office Facility  
**IC**—Installation Commander  
**MAJCOM**—Major Command  
**NID**—National Interest Determination  
**OPR**—Office of Primary Responsibility  
**OPSEC**—Operations Security  
**PCL**—Personnel Security Clearance  
**PCO**—Procuring Contracting Officer  
**PM**—Program Manager  
**RFB**—Request for Bid  
**RFP**—Request for Proposal  
**RFQ**—Request for Quote  
**SAF**—Secretary of the Air Force  
**SAP**—Special Access Program  
**SAV**—Staff Assistance Visit  
**SCI**—Sensitive Compartmented Information

**SM**—System Manager

**SPO**—System Program Office

**SOO**—Statement of Objectives

**SOW**—Statement of Work

**VGSA**—Visitor Group Security Agreement

### *Abbreviations and Acronyms*

**CAGE**—commercial and government entity (code)

**DTIC**—Defense Technical Information Center

**FAC**—functional area chief

**FOUO**—for official use only

**IA**—information assurance

**ISPM**—information security program manager

**NCC**—network control center

**PWS**—performance work statement

**SATE**—security awareness, training, and education

**SSO**—special security office

### *Terms*

**Classified Contract**—Any contract that requires or will require access to classified information by the contractor or the employees in the performance of the contract. A contract may be classified even though the contract document itself is not classified.

**Cleared Facility**—A non-government owned and operated industrial, educational, commercial, or other facility for which DOD has made an administrative determination (from a security viewpoint) that the entity is eligible for and requires access to classified information of a certain category (Confidential, Secret, or Top Secret).

**Cognizant Security Office**—The designated Department of Defense (DOD) agency responsible for industrial security program administration. The Secretary of Defense (SECDEF) has designated the Defense Security Service (DSS) to perform this function. The Director of DSS has further delegated this responsibility downward within the agency. DSS Regional Directors provide industrial security administration for DOD contractor facilities located within their respective geographical area. One exception, for which ISPM has responsible, is DOD contractors on Air Force installation who have been designated as “visitor groups.” When used, the language “Cognizant Security Office” (CSO), always refers to DSS or an entity thereof.

**Information Security Program Manager (ISPM)**—This AF entity implements and administers the installation’s information, personnel and industrial security programs. The ISPM is responsible for supervising and overseeing on-base contractor’s security programs and/or operations.

**Installation**—An installation is an area in which the Air Force holds a real property interest or real

property over which the Air Force has jurisdiction by agreement with a foreign government or by right of occupation. The term installation also includes all auxiliary off-base or detached installations under the jurisdiction of the commander of the primary installation.

**Integrated Visitor Groups**—An on-base contractor operation, cleared per the NISP or ISR, that requires access to classified information and operates under the direct control/supervision of the Air Force. The integrated visitor group is authorized to function in accordance with DOD 5200.1-R and AFI 31-401 per the VGSA. The Air Force maintains control of all classified and provides day-to-day supervision over this type of contractor operation. It basically differs from the on-base cleared facility because of its close interaction and/or relationship with the AF organization it supports.

**Interim Facility Security Clearances (Interim FCL)**—Interim FCL are temporary, limited company security clearances established by the DSS. It does not permit access to Restricted Data, COMSEC, North Atlantic Treaty Organization (NATO), SCI, SAP, or Arms Control and Disarmament Agency classified Information. However, if an interim Top Secret FCL is issued, the contractor may access such information at the level of Secret and Confidential. Interim FCLs may not be appropriate for all contractual needs and are not available for all sponsored companies.

**Intermittent Visitor**—A contractor or company, cleared per the NISP or ISR, that require “entry” to an Air Force installation for brief periods of time on a scheduled or on call basis to perform contractual duties. An intermittent visitor’s presence on an installation usually does not exceed 90 consecutive days.

**Invalidation**—A condition at a cleared facility caused by changed conditions or performance under which the facility may no longer be eligible for an FCL unless the facility promptly initiates appropriate corrective actions.

**Major Discrepancy**—A condition, which resulted in or could reasonably be, expected to result in the loss or compromise of classified information.

**On-Base Cleared Facility**—An on-base contractor operation cleared under the provisions of the NISP and established at the discretion of the IC per DOD 5220.22-R. These entities operate under NISPOM guidance and the ISPM has been designated by the IC to provide security oversight.

**Reciprocity**—A reciprocal condition, relationship, mutual or cooperative agreement, between two or more agencies, components, or departments agreeing to recognize and accept the efforts (requirements, procedures, actions, etc.) of the other in exchange for the same compensation.

**Visitor Group**—Any on-base contractor operation, cleared per the NISP or ISR, that requires access to classified information. The installation commander determines their “official” on-base designation. (NOTE: All on-base contractor operations are considered “visitor groups,” per this AFI. The IC assesses and evaluates the working relationship and interactions between the visitor group and AF activity to determining their “official” designation, i.e., cleared facility, integrated visitor group or intermittent visitor).

**Visitor Group Security Agreement**—A documented and legally binding contractual agreement between an Air Force activity and a DOD contractor whereby the contractor commits to complying with, rendering or performing specific security tasks or functions for compensation. The VGSA attest to and certifies the existence of such an agreement, including applicable changes and amendments, attachments, supplements and exhibits.

**ATTACHMENT 2 (ADDED-AETC)****INSTRUCTIONS FOR COMPLETING A BASIC DD FORM 254**

**A2.1. (AETC)** These instructions apply to contracting officers, procurement officials, FACs, program managers, and project managers responsible for creating and updating DD Forms 254. A DD Form 254 will be prepared for each contract requiring a contractor to have access to classified information during solicitation or performance phases.

**A2.2. (AETC)** DD Forms 254 will be typewritten or computer generated; facsimiles (fax) will not be used. A DD Form 254 is part of the contract presented to the contractor and must be legible. It is a binding agreement that provides the contractor security classification guidance for contract performance.

**A2.3. (AETC)** The following guidance is for use with the corresponding block on DD Form 254:

**A2.3.1. (AETC) Item 1a.** Enter the highest level of access to classified information needed during the contract. Use only Top Secret, Secret, or Confidential. Do not confuse this clearance with the contractor's home office facility clearance.

**A2.3.2. (AETC) Item 1b.** For cleared contractor facilities, list the level of safeguarding required (Top Secret, Secret, or Confidential). This level may not be higher than shown in Item 1a. This item does not normally apply to onbase integrated visitor groups. If the contractor is not required to store classified material, enter "NA" or "None."

**A2.3.3. (AETC) Item 2.** Place an "X" in only one item. Item 2a is for prime contracts issued by the government, item 2b is only for use by the prime contractor to award subcontracts, and item 2c is for the solicitation phase of a contract. The contracting office will issue the solicitation number and enter the due date (the date bids are due to the contracting officer). When the contract is awarded, a new DD Form 254 will be prepared by the FAC, program manager, or project manager and issued with the contract number entered in item 2a.

**A2.3.4. (AETC) Item 3.** Place an "X" in only one item. Item 3a is used when the original DD Form 254 is issued. (Also enter the original date.) The original date is unchanged on each subsequent revision. When a revised DD Form 254 is issued, place an "X" in item 3b and show revision number and revision date. Each time a revision is issued, give it a sequential number. Place an "X" in Item 3c for a final DD Form 254 and enter the date the final DD Form 254 is issued. A final DD Form 254 is not required unless (and until) the contractor is authorized or denied authority to retain classified information or has been granted an extension of retention.

**A2.3.5. (AETC) Item 4.** If this is a follow-on contract, place an "X" in the "yes" block and enter the preceding contract number in the space provided. If this is not a follow-on contract, place an "X" in the "no" block.

**A2.3.6. (AETC) Item 5:**

**A2.3.6.1. (AETC)** Place an "X" in the "no" block if this is not a final DD Form 254. Only issue a final DD Form 254 after the contracting officer determines the disposition of classified material and after contract completion. (The contractor may be allowed to retain classified information or may be required to return the information to the Air Force.)

**A2.3.6.2. (AETC)** Place an "X" in the "yes" block if this is a final DD Form 254. If the contractor is authorized to retain classified information, list the date the contractor requested retention and the period of time the contractor is authorized retention. **NOTE:** Visitor group contractors are not authorized to retain classified information past the contract's completion.

**A2.3.7. (AETC) Item 6.** This item is not used during the solicitation phase of a contract.

**A2.3.7.1. (AETC)** When a contract is awarded, enter the contractor's mailing address in item 6a; that is, the address used to send classified material to the contractor. The FAC, program manager, or project manager will verify this address with the Defense Security Service-Operating Center Columbus (DSS-OCC). The DSS-OCC address and phone number are located in DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*.

**A2.3.7.2. (AETC)** Enter the CAGE code of the cleared facility in item 6b. The FAC, program manager, or project manager will obtain the CAGE code from the DSS-OCC when verifying the contractor's physical address.

**A2.3.7.3. (AETC)** In item 6c, list the DSS regional office that has cognizance over the contractor. Spell out the full address; do not use abbreviations. The cognizant security office is always the director of industrial security who has industrial security jurisdiction over the geographical area where the contractor is located. No other activity should be shown in this item.

**A2.3.8. (AETC) Item 7.** This item is only used by the prime contractor to award subcontracts.

**A2.3.9. (AETC) Item 8.** This item is used only when contract performance is in a different location than identified in item 6. If the contractor is a visitor group on a DoD installation, show where the onbase performance will occur. **NOTE:** If the contract performance location is the same location as identified in Item 6a, put the following statement: "Same as Item 6a." Do not put "NA" in item 8a as your answer.

**A2.3.10. (AETC) Item 9.** Enter a short, concise, unclassified title or explanation of the contract.

**A2.3.11. (AETC) Item 10.** Mark each item either "yes" or "no." (See paragraphs [A2.3.12.](#) through [A2.3.21.](#) for further explanation.)

**A2.3.12. (AETC) Item 10a.** If the contractor does not require access to COMSEC information, mark this item "no." Mark the item "yes" if:

**A2.3.12.1. (AETC)** Accountable COMSEC information is required for contract performance. This includes hard copy or electronic storage or transmittal of COMSEC material.

**A2.3.12.2. (AETC)** The contract involves computer system operations; for example, operation of a wing network control center (NCC) where cryptographic equipment is installed and the associated COMSEC material is controlled and accounted for by the contractor. **NOTE:** For contracted NCC operations on AETC installations, the local communications squadron will inspect the contractor. In this case, check items 10f and 15 "yes" and state the following in item 15: "XXX Communications Squadron inspects contracted NCC operations. AETC CSS/SCNS (AETC COMSEC Manager) will biennially assess the contractor when the squadron is required to control and account for COMSEC material/equipment."

**A2.3.13. (AETC) Items 10b, 10c, and 10d.** These items apply to information covered by the Atomic Energy Act of 1954. Although this is not DoD information, special markings and briefings are

required. If the contract does not cover nuclear weapons or nuclear weapons design information, mark these items "no." If this information is required, mark appropriate items "yes."

**A2.3.14. (AETC) Item 10e(1).** If this item is marked "yes," contact the local SSO for the information required in item 14. Coordinate the form with the SSO before coordinating with the ISPM. Also mark items 14 and 15 "yes." Identify security requirements for SCI in item 14 or by attachment to the form (for example, Attachment 1, SCI Security Requirements). In item 15, identify the SSO as the activity conducting inspections. Ensure instructions for SCI include total number of the SCI billets required and the contract monitor's name, title, organization, telephone number, and signature. Also provide the contract expiration date.

**A2.3.15. (AETC) Item 10e(2).** Mark this item "yes" if access is required to non-SCI intelligence information. Check item 14 "yes" and provide security guidance or identify the attachment to the DD Form 254 that lists non-SCI intelligence security requirements (for example, Attachment 2, Non-SCI Intelligence Security Requirements).

**A2.3.16. (AETC) Item 10f.** A "yes" marked in this item requires explanation in item 14. For example, list the special access security directive that outlines security requirements for the special access program. If DSS is "carved out of" inspection responsibilities, list elements or areas DSS is carved out of and the activity responsible for the inspection. This also includes COMSEC.

**A2.3.17. (AETC) Item 10g.** Mark this item "yes" if access to NATO classified information is required. In item 13, list the level of access required and, if possible, state the documents or information required.

**A2.3.18. (AETC) Item 10h.** Mark this item "yes" if access is required to foreign government classified information. In Item 13, list the level of access required for foreign government information and, if possible, foreign government documents required for contract performance.

**A2.3.19. (AETC) Item 10i.** This item will always be answered "no" because limited dissemination information is no longer an approved DoD program.

**A2.3.20. (AETC) Item 10j.** If this item is marked "yes," provide the contractor specific guidance in item 13 or identify the attachment to the DD Form 254 that provides for official use only (FOUO) guidance (for example, Attachment 3, FOUO Guidelines).

**A2.3.21. (AETC) Item 10k.** If there is contract performance on base, place the following statement in this item: "Notification of Government Security Activity is required by the Federal Acquisition Regulation (FAR) 52.204-2."

**A2.3.22. (AETC) Item 11.** Mark each item either "yes" or "no." **NOTE:** In the first three items, only one may be marked "yes;" the others must be marked "no."

**A2.3.23. (AETC) Item 11a.** Note the word "only" in this item. This means there will be no access to classified information at the contractor's facility. The contractor will not be required to have any safeguarding capability in item 1b. If item 11a is marked "yes," items 11b, 11c, 11d, and 11k will be marked "no." Mark the remaining items "yes" or "no" as required.

**A2.3.24. (AETC) Item 11b.** This item means the contractor will *receive*, but not *generate*, classified information. If item 11b is checked "yes," mark items 11a and 11c "no."

**A2.3.25. (AETC) Item 11c.** This item means the contractor will receive and generate classified material and will receive security classification guidance for performance of the contract. If the "yes"

item is marked, security classification guidance must be provided to the contractor in item 13, as an attachment to DD Form 254, or under separate cover. If item 11c is marked "yes," mark items 11a and 11b "no."

**A2.3.26. (AETC) Item 11d.** If this item is marked "yes," indicate in item 14 (or item 13 if item 14 is filled) any secure open storage areas required. If hardware is involved, indicate how much, its size, and the point at which it becomes classified.

**A2.3.27. (AETC) Item 11e.** If this item is marked "yes," see DoD 5220.22-R for statements required in Item 13.

**A2.3.28. (AETC) Item 11f.** If the contractor performs outside the CONUS, in Item 13 list the city and country where the contractor will perform services. In item 15, list the ISPMs responsible for contractor inspections.

**A2.3.29. (AETC) Item 11g.** A "yes" marked in this item authorizes the contractor to use the services of the Defense Technical Information Center (DTIC). Contractors performing service-type contracts normally don't need DTIC access.

**A2.3.30. (AETC) Item 11h.** Mark this item "yes" if the contractor is responsible for managing a COMSEC account. Mark this item "no" if the contractor will require access to COMSEC material through an Air Force COMSEC account.

**A2.3.31. (AETC) Item 11i.** When this item is marked "yes," the contractor will perform classified computer processing. This item does not apply to a maintenance service contract where the contractor is not in control of the computer system classified operation or where the contractor provides operators, etc., for a service contract. When this item is checked "yes," Chapter 8 of DoD 5220.22-M applies. (**NOTE:** For Air Force contractor visitor groups, refer to AFI 33-202 for specific guidance.) If the requirement to perform classified AIS processing is on an AETC installation, extract specific requirements from AFI 33-202 and enter them in item 13. When the item is checked "yes," EMSEC requirements must be considered. Coordinate the DD Form 254 with the chief of the IA Office to obtain current EMSEC guidelines to be listed in item 13.

**A2.3.32. (AETC) Item 11j.** When this item is marked "yes," put an explanation in item 13, indicating where in the security portion of the contract document the data item description is listed for contractor performance of operations security (OPSEC).

**A2.3.33. (AETC) Item 11k.** Mark this item "yes" if the contractor is authorized to use the Defense Courier Service.

**A2.3.34. (AETC) Item 11l.** Use this item to add additional information not covered elsewhere in item 11.

**A2.3.35. (AETC) Item 12.** Normally, put an "X" in the "Through" block and specify HQ AETC/PAN on HQ AETC-generated DD Forms 254 or specify the local PA on DD Forms 254 created at AETC installations. For special access, SCI, and other intelligence information, do not list HQ AETC/PAN or the local PA. Instead, work with the local ISPM and the FAC, program manager, or project manager to determine who, if anyone, should be listed in Item 12 or if the comment "No Release Authorized" should be used.

**A2.3.36. (AETC) Item 13.** This is the most important part of the DD Form 254. When completing this item, be sure to consider all the information below:

**A2.3.36.1. (AETC)** Put yourself in the contractor's place and try to determine what guidance will be needed to properly protect the classified information to be furnished or generated under the contract. Following are some of the questions to consider when preparing guidance for a contract:

**A2.3.36.1.1. (AETC)** What classified information will the contractor need to perform this contract?

**A2.3.36.1.2. (AETC)** What guidance will the contractor need to protect the classified information?

**A2.3.36.1.3. (AETC)** Is there more than one classification guide that will provide guidance to the contractor?

**A2.3.36.1.4. (AETC)** Will classified hardware be furnished to or generated by the contractor?

**A2.3.36.1.5. (AETC)** What information makes the hardware classified? Will the hardware being generated require classification? At what stage in its production does the hardware become classified?

**A2.3.36.1.6. (AETC)** What unique characteristics are involved that need protection? Are there design features that require protection? What technical information requires protection? What breakthroughs would be significant if achieved in a research and development (R&D) effort? Are there some performance limitations that require protection?

**A2.3.36.2. (AETC)** Use this item to identify applicable guides; provide narrative guidance that identifies the specific types of information to be classified; provide appropriate downgrading or declassification instructions; provide any special instructions, explanations, comments, or statements required for information; and/or clarify any other items identified on the DD Form 254. Each contract is unique in its performance requirements. Do not try to follow a format or provide all the guidance in this item. Give reasons for the classification. Write the guidance in plain English. Use additional pages as necessary to expand or explain the guidance.

**A2.3.36.3. (AETC)** DD Form 254, with its attachments and incorporated references, is the only authorized means of providing security classification guidance to a contractor. It should be as specific as possible and should only include information that pertains to the contract for which it is issued. If the package contains references to internal directives and instructions, provide the contractor with the documents. Provide the contractor with any and all documents referenced or cited in this item, either as attachments or forwarded under separate cover if classified. The requirements of DoD 5220.22-M or its supplements should not be extracted and included in a DD Form 254. The DoD 5220.22-M provides safeguarding requirements and procedures for classified information, not security classification guidance. (**NOTE:** For Air Force contractor visitor groups, refer to DoD 5200.1-R and AFI 31-401 for safeguarding requirements.) Security classification guidance provides detailed information about what information requires classification, the level of classification to assign, and the downgrading or declassification instructions that apply to the information or material generated in the performance of the contract.

**A2.3.36.4. (AETC)** It is difficult to prepare security classification guidance that covers all of the performance requirements of a classified contract. It is even more difficult to prepare guidance that can be understood and implemented by the contractor. If at all possible, encourage the contractor to help prepare guidance and provide comments and/or recommendations for changes in the guidance that has been provided. Only through effective communication with the contractor

can you achieve understandable guidance and ensure the proper classification and protection of the information generated in the performance of the contract.

**A2.3.36.5. (AETC)** Annotate the name, grade, organization, and signature of all coordinating and review officials in this item.

**A2.3.37. (AETC) Item 14.** Mark this item "yes" any time security requirements are imposed on a contractor that are in addition to the DoD 5220.22-M or its supplements. (**NOTE:** Air Force contractor visitor groups will comply with DoD 5200.1-R and AFI 31-401.) If this item is marked "yes," it requires incorporation of the additional requirements in the contract document. If the contractor will be a visitor group on an AETC installation, mark this item "yes" and enter the following statement: "A visitor group security agreement (VGSA) will be executed between the installation commander and the contractor."

**A2.3.38. (AETC) Item 15.** Mark this item "yes" any time the cognizant security office (known as DSS) is relieved of inspection responsibility for all or part of the contract. If DSS is relieved of inspection responsibility, list all or portions of the program DSS is relieved of and the name of the activity tasked with inspection responsibilities. Also see item 10f.

**A2.3.39. (AETC) Item 16.** Enter the name, title, telephone number, address, and signature of the project or program manager responsible for certifying that the security requirements are complete and adequate. This person will also answer questions that arise on DD Form 254.

**A2.3.40. (AETC) Item 17.** As a contractual document, DD Form 254 is distributed with the contract to all marked addresses. Ensure all base ISPMs and MAJCOM information security divisions are listed when the contract performance is on a DoD installation. If necessary, use an attachment to DD Form 254 to list the addresses. If the contract involves the NCC or the control and accounting of COMSEC material or equipment, include the chief of the IA office. If the contract involves SCI information, include the SSO with security inspection responsibilities. If the contract involves SCI information and requires SCI billets, include the user agency SSO, the parent MAJCOM, and the Air Force Central Adjudication Facility, 229 Brookley Ave, Bolling AFB, Washington D. C. 20332-7040.

**ATTACHMENT 3 (ADDED-AETC)****INSTRUCTIONS FOR COMPLETING A TASK ORDER DD FORM 254**

**A3.1. (AETC) General.** A FAC, program manager, or project manager may be required to generate a task order DD Form 254. There are a few minor differences between a basic DD Form 254 and a task order DD Form 254. A basic contract DD Form 254 is created to list basic security requirements for classified information. If specific tasks arise, then a separate task order DD Form 254 is created to provide specific guidance for the task, as follows:

**A3.1.1. (AETC) Item 2a.** Write the contract number and annotate a locally created task order number (for example, contract number \_\_\_\_, task order #1).

**A3.1.2. (AETC) Item 13.** Insert the following statement: "This task order requires the following security classification guide which differs from the basic guidance. The specific classification guidance or security classification guide and date of classification guide will be used to include all revisions and changes thereto." **NOTE:** Identify the specific security classification guidance or security classification guide, title, and date.

**A3.1.3. (AETC) Item 15.** The task order may require portions of the contract be performed on a DoD installation. Ensure the following statement is in item 15 of the basic DD Form 254 as well as the specific task order DD Form 254: "Work performance will take place at (installation). The DSS is relieved of industrial security inspection responsibility at (installation). The ISPM provides oversight of the onbase contractor."