

**BY ORDER OF THE COMMANDER  
AIR EDUCATION AND TRAINING  
COMMAND**



**AIR FORCE INSTRUCTION 31-601  
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 AETC/SFI (Mr J. Helfenstein)  
Supersedes AFI 31-601/AETC Sup 1,  
10 June 1996

Certified by: HQ AETC/SFI (Mr B. Kilgore)  
Pages: 12  
Distribution: F

---

**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.**

1.6.1.2. 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.

1.6.1.4. 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.

1.6.2.2. 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.

1.6.2.5. 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.

1.6.5.1. 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.

1.7. 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).

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

3.2.3. 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.

4.1.2. 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.

4.3.2. 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.

4.4.2. 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.

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

6.2.1. 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.)

6.2.3. 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.

7.1. 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*.

7.3.2. 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.

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

9.1.1.2.1. 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 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) 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. 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) COMPUSEC procedures are as follows:

9.1.2.1.1. 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. 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. 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) EMSEC procedures are as follows:

9.1.2.2.1. 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. Contractors must follow EMSEC countermeasures established by the wing EMSEC manager.

9.1.2.2.3. 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.

9.1.4. 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.

10.2. 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.

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

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

Attachment 1, References. The following are added:

### ***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*

Attachment 1, Abbreviations and Acronyms. The following are added:

### ***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

**Attachment 2 (Added)****INSTRUCTIONS FOR COMPLETING A BASIC DD FORM 254**

**A2.1.** 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.** 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.** The following guidance is for use with the corresponding block on DD Form 254:

**A2.3.1. 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. 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. 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. 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. 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. Item 5:**

**A2.3.6.1.** 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.** 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. Item 6.** This item is not used during the solicitation phase of a contract.

A2.3.7.1. 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. 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. 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. Item 7.** This item is only used by the prime contractor to award subcontracts.

**A2.3.9. 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. Item 9.** Enter a short, concise, unclassified title or explanation of the contract.

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

**A2.3.12. 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. Accountable COMSEC information is required for contract performance. This includes hard copy or electronic storage or transmittal of COMSEC material.

A2.3.12.2. 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. 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. 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. 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. 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. 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. 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. Item 10i.** This item will always be answered "no" because limited dissemination information is no longer an approved DoD program.

**A2.3.20. 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. 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. 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. 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. 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. 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. 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. Item 11e.** If this item is marked "yes," see DoD 5220.22-R for statements required in Item 13.

**A2.3.28. 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. 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. 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. 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. 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. Item 11k.** Mark this item "yes" if the contractor is authorized to use the Defense Courier Service.

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

**A2.3.35. 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. 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. 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. What classified information will the contractor need to perform this contract?

A2.3.36.1.2. What guidance will the contractor need to protect the classified information?

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

A2.3.36.1.4. Will classified hardware be furnished to or generated by the contractor?

A2.3.36.1.5. 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. 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. 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. 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. 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. Annotate the name, grade, organization, and signature of all coordinating and review officials in this item.

**A2.3.37. 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. 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. 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. 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)****INSTRUCTIONS FOR COMPLETING A TASK ORDER DD FORM 254**

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

**A3.1.2. 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. 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."

RICHARD K. ELDARD, Colonel, USAF  
Director of Security Forces