

Security

INDUSTRIAL SECURITY

SUPPLEMENTATION. Local supplementation of this regulation is prohibited. The words "he" and "his" when used in this regulation represent both the masculine and feminine genders.

SUGGESTED IMPROVEMENTS. The proponent of this regulation is the office of the ACoFS, G2/DSEC. Users are invited to send comments and suggested improvements to Commander, III Corps and Fort Hood, ATTN: AFZF-DS-S.

OVERVIEW

		1
Purpose	<p>This regulation provides command guidance and policy concerning the implementation of the Defense Industrial Security Program (DISP) which is promulgated by</p> <ul style="list-style-type: none"><li>• DoD 5220.22-M, Industrial Security Manual (ISM), Mar 84</li><li>• DoD 5220.22-R, Industrial Security Regulation (ISR), Feb 84, and</li><li>• AR 380-49, Industrial Security Program, Apr 82.</li></ul> <p>(See Appendix A).</p>	1a
Applicability	<p>This regulation is applicable to all elements subordinate to</p> <ul style="list-style-type: none"><li>• Headquarters III Corps and Fort Hood</li><li>• tenant activities, and</li><li>• contractors using Fort Hood real estate and facilities while engaged in contracts which require the<ul style="list-style-type: none"><li>• use</li><li>• acquisition</li><li>• dissemination</li><li>• production, or</li><li>• storage of classified defense information, e.g.<ul style="list-style-type: none"><li>• CONFIDENTIAL</li><li>• SECRET, or</li><li>• TOP SECRET.</li></ul></li></ul></li></ul>	1b
Policy	<p>To accomplish a uniform industrial security program on Fort Hood, the following basic procedures are established:</p> <ul style="list-style-type: none"><li>• Contractors conducting business on Fort Hood will be subject to DoD and Fort Hood security procedures concerning the safeguarding of classified defense information and related activities. (Contractor internal security procedures are governed by the ISM unless modified by contract.)</li><li>• Only those security badges authorized by the Commander, Fort Hood, will be used by contractor personnel at Fort Hood.</li><li>• Only those security forces authorized or approved by the Commander, Fort Hood will be used by contractors at Fort Hood.</li><li>• The office of the ACoFS, G2/DSEC (AFZF-DS-S) is the proponent for the Industrial Security Program at Fort Hood.</li></ul>	1c
Definitions	<p>See Appendix B.</p>	1d

## RESPONSIBILITIES

2

Deputy  
DSEC

The Deputy DSEC will:

- Provide Command Policy guidance to assure security control of contractors performing classified contracts within the geographical jurisdiction of Fort Hood.
- Administer an effective DISP and ensure a proper interface with other Fort Hood activities.
- Resolve conflicts that occur within the commander's responsibility, subparagraph 1-108b, ISR.

2a

Chief,  
Industrial  
Security  
Branch,  
DSEC

The Chief, Industrial Security Branch, DSEC, will:

- Serve as a central point of contact for all industrial security matters pertaining to Fort Hood operations.
- Conduct security surveys and inspections of Fort Hood based contractors engaged in classified contracts in accordance with the ISR. Coordinate surveys and inspections of contractor
  - arms
  - ammunition, and
  - explosives under AR 190-11, with the Physical Security Section, Office of the Provost Marshal.
- Designate contractor operations within Fort Hood jurisdiction as
  - facilities
  - long term visitors
  - or visitors
    - consistent with size
    - complexity, and
    - tenure (visitor categories are contained in Section III, ISR).
- Operate a centralized visitor control and security badging service for the ISP.
- Conduct industrial security training for contractor personnel and Fort Hood activities as necessary.
- Maintain a copy of the DD Form 254, Contract Security Classification Specification, and Standard Practice Procedures (SPP) for each contractor tenanted at Fort Hood.
- Maintain reports of security inspections of contractors engaged in classified contracts and tenanted at Fort Hood.
- Participate in the planning and negotiations of contracts to be let at Fort Hood to determine security requirements and compliance with the ISM and ISR.
- Provide contractor personnel security clearance information to Fort Hood and tenant activities as necessary.
- Conduct the Industrial Security Classification Management Program at Fort Hood as follows:
  - Review all original, revised, and final DD Forms 254, prepared by Fort Hood activities, including tenant organizations, for contracts to be let at Fort Hood.

Continued on next page

Chief,  
Industrial  
Security  
Branch,  
DSEC  
(Continued)

- Ensure that classification guidance furnished to contractors by Fort Hood activities, including tenants, is periodically reviewed in accordance with the requirements established by Section VII, ISR, and that revised or final DD Forms 254 are issued, as appropriate.
- Maintain copies of the classification guidance furnished to contractors by Fort Hood procurement activities, including tenants.
- Advise Fort Hood procurement activities, including tenants, of requirements that impose a different or greater standard of security than that established by the ISM.
- Ensure that each contractor promptly reports to DSEC all incidents which involve
  - espionage
  - sabotage
  - subversive activity
  - loss
  - compromise, or
  - suspected compromise of classified defense information.
- Monitor the conduct of administrative inquiries by contractors of their security violations and conduct additional investigations to expand or supplement the contractor's inquiry.
- Conduct preliminary investigations of non-Fort Hood contractor security violations that are Fort Hood related and report the results to the appropriate cognizant security office.

2b

Fort Hood  
Contracting  
and Procure-  
ment Activ-  
ities

Fort Hood contracting and procurement activities, including those of tenants, will:

- Notify DSEC to participate in long range commercial activity planning to ensure advance industrial security planning.
- Ensure that Contractors of Record are made aware of their industrial responsibilities and of the necessity of maintaining effective liaison with DSEC.
- Submit requests for verification of facility clearance and safeguarding capability as necessary to DSEC prior to releasing classified information to offerors bidding on a classified contract.
- Submit requests for contractor facility clearance to DSEC as required for a contractor to participate in procurement action that requires or will require access to classified defense information.
- Inform DSEC of the
  - completion
  - termination, or
  - default of classified contracts.
- Request participation by DSEC, as necessary, in the close out inspections of contractor facilities at Fort Hood and location other than Fort Hood to ensure the proper disposition of classified defense materials.
- Ensure that all original, revised, and final DD Forms 254 have been reviewed by DSEC prior to being issued to contractors and that DSEC has been provided with a copy of each form that has been approved by the contracting officer.

Continued on next page

Fort Hood  
Contracting  
and Procure-  
ment Activ-  
ities  
(Continued)

- Ensure that the original Fort Hood user activity, including tenants, conduct a review of all classified defense material requested for retention by a contractor at the termination of a contract to assist in determining the level of classified material that could be furnished to the contractor, if the contracting officer approves the request. Defense Investigative Service will make the final determination concerning retention.

2c

Directors,  
Staff Office  
Chiefs, and  
Heads of  
All Fort Hood  
Activities

Directors, staff office chiefs, and heads of all Fort Hood activities will:

- Ensure advance industrial security planning by notifying DSEC of:
  - Intentions to tenant or become involved in any way with a contractor utilizing or visiting Fort Hood with the exception of unclassified contracts dealing with food and beverage service. This includes the intention to invite a contractor or representative to visit Fort Hood. DSEC will determine any security implications.
  - Plans to change the nature of or expand the scope of a tenant contractor's operation.
  - Classified defense program or projects that will require contractor personnel to visit Fort Hood, including the fielding or testing of
    - weapons
    - systems
    - equipment, or
    - any security related construction or remodeling.
- Provide input as necessary for the preparation of DD Form 254 in accordance with instructions contained in the ISR or furnished by Fort Hood contracting or procurement offices or DSEC.
- Conduct periodic review in accordance with the requirements of Section VII, ISR, of the classification guidance furnished to contractors.
- Perform the following security actions, as necessary, for long term visitor facilities designated by DSEC as being the responsibility of the using Fort Hood activity
  - Ensure contractor has security classification guidance.
  - Ensure contractor has adequate classified storage facilities.
  - Other security services deemed necessary.
- Ensure that contractor visitors to the activity know and comply with applicable requirements of this regulation, including
  - visitor control
  - security badging
  - range overflight, and
  - photography requirements.
- Ensure that Type A Consultants to their activity:
  - Have executed a Type A Consultant Certificate with the user activity.
  - Are provided with adequate classification guidance.
  - Are furnished copies or organization security SOP's and are otherwise made aware of Fort Hood security requirements.
- Ensure contractor visitors requiring access to classified information check in with DSEC prior to conducting business (visitor should have a dated visitor badge).

2d

Directors or  
Chiefs of  
Fort Hood  
Tenant  
Organizations

Directors or chiefs of Fort Hood tenant organizations will:

- Accomplish all of the actions as stated above.
- Ensure that DD Forms 254, which are to be issued to contractors by procurement activities other than at Fort Hood, include DSEC in item 12 and in the distribution block when the contracts for which the forms are being issued will require performance by the contractors at Fort Hood.

2e

Contractors

Contractors:

- Having facility security clearances or tenure at Fort Hood under long term visit agreements will obtain guidance in industrial security matters from DSEC.
- Will comply with
  - ISM
  - ISR, and
    - Fort Hood industrial security regulations
    - policies, and
    - procedures.
- Having a facility security clearance or occupying premises on Fort Hood as a long term visitor will formulate a security SPP manual governing their internal security operations.
  - One draft copy of the proposed SSP will be forwarded, through the Contracting Officer, to DSEC for review prior to publication.
  - Upon publication, one copy of the SPP will be forwarded for retention.
- Will appoint a security manager to supervise security measures necessary to ensure compliance with security directives and for the safeguarding of classified information.
- Will promptly notify DSEC of changes affecting the contractor's security operations such as
  - changes in personnel and
  - location of classified material.
- Having facility security clearance or tenure at Fort Hood under long term visit agreements will submit reports as required by paragraph 6 and 7 of the ISM to DSEC.
- Will request personnel security clearances in accordance with the ISM, except as noted below:
  - Request for personnel security clearances for
    - officers,
    - directors, and
    - executive personnel will be forwarded to DSEC.
- Requests for interim security clearances for additional contractor employees required for performance of Fort Hood administered or awarded contracts will be routed through the appropriate Government Contracting Officer to DSEC.
- Will inform DSEC of the
  - name
  - phone number, and
  - address of their security office.

2f

Visitor  
Representing  
Contractors

Visitor representing contractors will:

- Provide request for visit and security clearance verification on contractor letterhead stationary for receipt at DSEC 5 working days prior to the visit.
- Report to DSEC upon arrival to be issued a dated, disposable badge.
- Identify their Fort Hood point of contact including:
  - Name,
  - Organization,
  - Building number or area/vicinity, and
  - Local telephone number.
- State the purpose of the visit in simple terms and the classification of information to which they will require access.
- Short notice visit requirements may be accommodated telephonically, provided written verification is forwarded in a timely manner.
- The III Corps and Fort Hood Industrial Security point of contact may be reached by:
  - Commercial (817) 287-3157 or 4706
  - AUTOVON 737-3157 or 4706
  - FTS 747-737-3157 or 4706
  - Commander  
III Corps and Fort Hood  
AF2F-DS-S (Industrial Security)  
Fort Hood, Texas

2g

FOR THE COMMANDER:



R. A. KOLIN  
COL, AGC  
Adjutant General

2 APPENDICES

- A - Synopses of Implementing Regulations.
- B - Definitions.

DISTRIBUTION:

IAW FH Form 1853, C  
Plus: HQ FORSCOM, ATTN: AFIN-CSC (2)  
AP2F-DS-S  
AG-PURS (100)  
AG-AO (2)

HARRY D. PENZLER  
Brigadier General, USA  
Chief of Staff

## APPENDIX A. Synopses of Implementing Regulation

The security of the US depends in part on the proper safeguarding of classified information released to industry. The objective of the DoD Industrial Security Program is to assure the safeguarding of classified information in the hands of US industrial organizations, educational institutions, and all organizations and facilities used by prime and subcontractors. A brief synopsis of applicable regulations cited in paragraph 1, Purpose, are as follows:

a. DoD 5220.22-M, Industrial Security Manual for Safeguarding Classified Information, contains detailed security requirements to be followed by US contractors for safeguarding classified information. It is a companion publication to the Industrial Security Regulation.

b. DoD 5220.22-R, Industrial Security Regulation, is authorized by the Secretary of Defense under the authority of the National Security Act of 1947, as amended, and is established as a DoD regulation under the authority of DoD Directive 5220.22, DoD Industrial Security Program. It sets forth policies, practices, and procedures of the DoD Industrial Security Program used internally by the DoD to ensure maximum uniformity and effectiveness in its application throughout industry. The authority granted the installation commander to implement the Industrial Security Program is found in paragraph 1-108, which states substantially as follows:

The Commander or Head of a User Agency installation shall provide security supervision of contractors and their employees located on the installation. The Commander may elect to declare the contractor activity a facility and request the Defense Investigative Service (DIS) to perform all security functions provided for in the regulation, or notify DIS that he has elected to perform the actions detailed in that paragraph. If the activity does not qualify as a facility and is subsequently declared a visitor, the responsible for the security functions detailed in that paragraph.

c. AR 380-49, Industrial Security Program, implements DoD Directive 5220.22, DoD Industrial Security Program, and DoD 5220.22-R, Industrial Security Regulation. Paragraph 10 of this regulation states in substance that the installation Commander will provide for the security of classified contracts performed on his installation, unless he has requested that DIS perform this service. Even if the Commander has relinquished his authority in this area, he continues to retain overall responsibility for the security of the installation.

## APPENDIX B. DEFINITIONS

1. **CLASSIFIED CONTRACT.** Any contract that requires (or will require) access to classified defense information (CONFIDENTIAL, SECRET, TOP SECRET) by the contractor or his employees in the performance of the contract. (A contract may be a classified contract even though the contract document is not classified.)
2. **CLASSIFICATION GUIDES.** Guidance issued or approved by an original TOP SECRET classification authority that identifies information or material to be protected from unauthorized disclosure; it also specifies the level and duration of classification assigned or assignable to such information or material under authority of Executive Order 12356. Classification guides are provided to contractors by DD Form 254.
3. **CLASSIFIED DEFENSE INFORMATION.** Information or material that is owned by, and produced by, for, or under the control of the US Government (pursuant to E. O. 12065) or prior orders to require protection against unauthorized disclosure, and is so designated.
4. **COMMUNICATIONS SECURITY (COMSEC).** The protection resulting from the application of cryptosecurity, transmission security, and emission security measures to communications and from the application of physical security measures to COMSEC information. These measures are taken to deny unauthorized persons information of value, that might be derived from the possession and study of such communications, or to ensure the authenticity of such communications.
5. **COMMUNICATIONS SECURITY (COMSEC) INFORMATION.** All information concerning COMSEC and all material (documents, devices, maintenance manuals, and equipment or apparatus) including Cryomaterial associated with the security or authenticity of telecommunications.
6. **COMPROMISE.** The disclosure of classified defense information to persons not authorized access to it.
7. **COMPROMISING EMANATIONS.** Unintentional data-related or intelligence-bearing signals which, if intercepted and analyzed, disclose the classified defense information transmitted, received, handled, or otherwise processed by electrically operated information processing equipment or systems.
8. **CONFIDENTIAL.** The designation applied to information or material the unauthorized disclosure of which could reasonably be expected to cause identifiable damage to the national security.
9. **CONTRACTING OFFICER.** A person who, in accordance with department or agency procedures, is currently designated a contracting officer, with the authority to enter into and administer contracts and make determinations and findings with respect to them or any part of such authority. The term also includes the authorized representative of the contracting officer acting within the limits of his authority. For purposes of this regulation and the ISM, the term "contracting officer" refers to the person at the purchasing office identified as the procuring contracting officer (PCO) and the person at a contract administration office identified as the administrative contracting officer (ACO).
10. **CONTRACTOR.** An entity (industrial, education, commercial, or other) that has executed a contract with a user agency or a DD Form 441 with a DoD agency or activity.
11. **CUSTODIAN.** An individual who has possession of (or is otherwise charged with) the responsibility for safeguarding or accounting for classified defense information.
12. **DOCUMENT.** Any recorded information, regardless of its physical form or characteristics (exclusive of machinery, apparatus, equipment, or other items of material). The term "document" includes, but is not limited to written material, whether handwritten, printed, or typed; photographs, negatives, exposed or printed films, and still or motion pictures; data processing cards or tapes; maps; charts; paintings; drawings; engraving; sketches; working notes and papers; reproduction of the foregoing by whatever process reproduced; and sound, voice, or electronic recordings in any form.
13. **FACILITY.** A plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components which, when related by function and location, forms an operating entity. (A business or educational organization may consist of one or more of these facilities). For purposes of industrial security, the term "facilities" does not include user agency installations.

14. **FACILITY SECURITY CLEARANCE.** An administrative determination that, from a security viewpoint, a facility is eligible for access to classified defense information of a certain category (and all lower categories).
15. **FOREIGN INTEREST.** Any foreign government or agency of a foreign government; any form of business enterprise organized under the laws of any country other than the United States, or its possessions; any form of business enterprise organized or incorporated under the laws of the United States, or a State or other jurisdiction of the United States, but owned or controlled by a foreign government, firm, corporation, or person. The term "foreign interest" also includes any natural person who is not a citizen or national of the United States. (An "immigrant alien" as explained below is excluded from the explanation of a foreign interest).
16. **IMMIGRANT ALIEN.** Any person lawfully admitted into the United States under an immigration visa for permanent residence.
17. **INDUSTRIAL SECURITY.** That portion of internal security that is concerned with the protection of classified defense information in US industry.
18. **INFORMATION SECURITY.** The result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure. Protection of this information is authorized by Executive Order or statute.
19. **NEED-TO-KNOW.** A determination made by the possessor of classified defense information that a prospective recipient, in the interest of national security, has a requirement for access to knowledge of (or possession of) the classified defense information, in order to perform tasks or services essential to the fulfillment of a classified contract or program approved by a user agency.
20. **NEGOTIATOR.** Any employee, in addition to the owners, officers, directors, and executive personnel (OODEPs), who requires access to classified defense information during the negotiation of a contract or the preparation of a bid or quotation pertaining to a prime or subcontract. The term "negotiator" may include, but is not limited to, accountants, stenographers, clerks, engineers, draftsmen, and production personnel.
21. **OFFICERS** (Corporation, association, or other types of business or education institution). Those persons in positions established as officers in the article or incorporation or bylaws of the organization.
22. **SECRET.** The designation applied to information or material, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include: disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; compromise of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.
23. **SECURITY.** The safeguarding of information classified TOP SECRET, SECRET, OR CONFIDENTIAL against unlawful or unauthorized dissemination, duplication, or observation.
24. **SECURITY COGNIZANCE.** The responsibility for acting for user agencies in the discharge of industrial security responsibilities.
25. **TOP SECRET.** The designation applied to information or material, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include: armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital material defense plans of complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific and technological development vital to national security.
26. **USER AGENCIES.** These agencies are explained below.
  - a. The Office of the Secretary of Defense (OSD) (including all boards, councils, staffs, and commands).
  - b. DoD agencies and departments of the Army, Navy, and the Air Force (including all of their activities).

27 July 1984

FH Reg 380-4

c. The National Aeronautics and Space Administration (NASA), General Services Administration (GSA), Small Business Administration (SBA), National Science Foundation, Environmental Protection Agency, and Federal Energy Administration.

d. The Department of State, Commerce, Treasury, Transportation, Interior, Agriculture, Health and Human Services, Labor, and Justice.

e. US Arms Control and Disarmament Agency and the Federal Emergency Management Agency (FEMA).