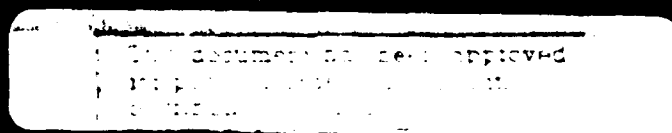
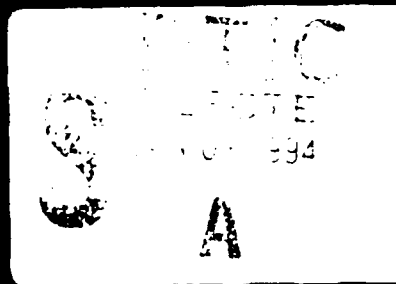
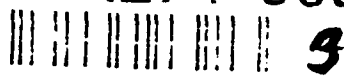
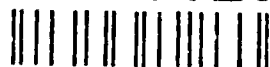


AD-A274 505



94-00261





December 3, 1980
NUMBER 5220.22

Department of Defense Directive

VSD(P)

SUBJECT: DoD Industrial Security Program

- References:
- (a) DoD Directive 5220.22, subject as above, December 1, 1976 (hereby canceled)
 - (b) Executive Order 10865, "Safeguarding Classified Information Within Industry," February 20, 1960, as amended by Executive Order 10909, January 17, 1961
 - (c) DoD Directive 5025.1, "Department of Defense Directives System," October 16, 1980
 - (d) DoD Directive 5220.6, "Industrial Personnel Security Clearance Program," December 20, 1976
 - (e) DoD Directive 5122.5, "Assistant Secretary of Defense (Public Affairs)," July 10, 1961

A. REISSUANCE AND PURPOSE

1. This Directive reissues reference (a) to implement reference (b) within the Department of Defense; assigns overall responsibility for policy and administration of the Defense Industrial Security Program (DISP); and ensures that classified information released to industry is properly safeguarded.

2. This Directive authorizes the following publications to be issued in accordance with the provisions of reference (c):

a. The Industrial Security Regulation (DoD 5220.22-R). This document prescribes detailed policies and procedures applicable to all user agencies in carrying out their responsibilities under the DISP.

b. The Industrial Security Manual for Safeguarding Classified Information (DoD 5220.22-M) and supplements thereto. This document is incorporated by reference into the Department of Defense Security Agreement and is part of the basic contract between the government and those contractors who require access to classified information.

(1) The document also is incorporated by reference into each contract, the performance of which requires access to classified information by the contractor or his or her employees.

(2) DoD 5220.22-M prescribes the specific requirements, restrictions, and other safeguards considered necessary in the interest of national security for the safeguarding of classified information.

c. The Industrial Security Letter. This document, which is issued as needed, provides guidance for industry in carrying out its responsibilities under the DISP.

d. Industrial Security Bulletin. This document, which is issued as needed, provides guidance to those in government having responsibilities related to the administration of the DISP.

B. APPLICABILITY

The provisions of this Directive apply to the Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff, and the Defense Agencies (hereafter referred to as "DoD Components").

C. POLICY

1. As provided in E.O. 10865 (reference (b)), the Secretary of Defense is authorized to prescribe, by regulation, such specific requirements, restrictions, and other safeguards as are considered necessary to protect:

a. Classified information provided to or within U.S. industry that relates to the bidding on, negotiation, award, performance, or termination of contracts with DoD Components.

b. Other classified information provided to or within industry that the Department of Defense has responsibility for safeguarding.

2. For the purposes of this Directive, U.S. industry includes any industrial, educational, commercial, or other entity and shall be referred to as "industry."

3. In addition, the Secretary of Defense is authorized to enter into agreements with any other department or agency of the Executive Branch to extend the regulations he prescribes to safeguard classified information provided to industry by these departments or agencies (D.I.F., below). Such other departments and agencies, as well as DoD Components, shall be referred to in this Directive as "user agencies."

4. The Department of Defense shall set forth policies, practices, and procedures to be followed by user agencies for the effective protection of classified information provided to industry, including foreign classified information the U.S. Government is obliged to protect in the interest of national security.

5. DoD Directive 5220.6 (reference (d)) established the standard and criteria for making security clearance determinations when persons employed in private industry require access to classified information.

6. DoD Directive 5122.5 (reference (e)) established the responsibility of the Assistant Secretary of Defense (Public Affairs) for the review of information pertaining to classified contracts before public disclosures by DoD contractors.

D. RESPONSIBILITIES

1. The Deputy Under Secretary of Defense (Policy Review) (DUSD(PR)) shall:
 - a. Be responsible for overall policy guidance and management oversight of the DISP.
 - b. Approve the issuance of changes to DoD 5220.22-M and DoD 5220.22-R.
 - c. Develop policies, plans, and programs for the DISP, and approve changes before issuance by the Director, Defense Investigative Service (DIS).
 - d. Coordinate with other offices in the OSD, as appropriate, all proposed policies, plans, and programs before referral for issuance by the Director, DIS.
 - e. Determine the effectiveness of the operation and administration of the DISP.
 - f. Upon request of other government departments or agencies, under E.O. 10865 (reference (b)), arrange, on behalf of the Department of Defense, to apply the provisions of the DISP to contractors of such departments or agencies, and render industrial security services required for the safeguarding of classified information released by such departments or agencies to industry. The Director, DIS, shall be kept currently informed of such agreements.
2. The Assistant Secretary of Defense (Public Affairs), unless otherwise delegated, shall review and clear information pertaining to classified contracts before public disclosures by DoD contractors. Contractors shall be required, as a contract obligation, to submit information materials described above according to DoD 5220.22-M.
3. The Director, Defense Investigative Service, under the general supervision of the General Counsel, DoD, shall administer the DISP as a separate program element on behalf of all DoD Components. In this capacity, the Director, DIS, shall assume security cognizance for all contractors and industrial facilities under the DISP on behalf of the Department of Defense, DoD Components, and user agencies, and shall provide investigative support, as required, for the administration of the DISP. In addition, the Director, DIS, shall:
 - a. Develop appropriate changes to maintain DoD 5220.22-R and DoD 5220.22-M, including supplements thereto, on a current and effective basis. Proposed changes to these documents shall be forwarded to the ODUSD(PR), ATTN: Director, Security Plans and Programs, for preliminary policy review.
 - b. Refer proposed changes to DoD 5220.22-R and DoD 5220.22-M to the DUSD(PR), ATTN: Director, Security Plans and Programs, and publish changes expeditiously, upon approval by the DUSD(PR).
 - c. Prepare, coordinate and publish the Industrial Security Letter and Bulletin on approval by the DUSD(PR), ATTN: Director, Security Plans and Programs.

d. Present on an annual basis, the James S. Cogswell Award to selected contractors in recognition of sustaining a superior security program for safeguarding classified information.


e. Budget, fund, and administer the DISP, including the appropriate field extensions. (The Defense Logistics Agency shall make appropriate funds available to DIS through FY 81.)

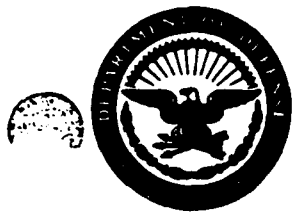
4. The Heads of DoD Components shall ensure that all their contracts requiring contractor access to classified information come within the purview of the DISP.

5. The Secretaries of the Military Departments shall provide counterintelligence support when requested.

E. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective October 1, 1980. Forward two copies of implementing documents to the Deputy Under Secretary of Defense (Policy Review) within 120 days.


W. Graham Claytor, Jr.
Deputy Secretary of Defense



DEFENSE INVESTIGATIVE SERVICE

1900 HALF ST. S.W.
WASHINGTON, D.C. 20324-1700

(1)

DoD 5220.22-R

December 4, 1985

FOREWORD

This regulation is issued under the authority of Department of Defense (DoD) Directive 5220.22, "DoD Industrial Security Program," December 8, 1980. Its purpose is to prescribe uniform procedures that ensure the safeguarding and protection of classified information made available to industry.

DoD 5220.22-R, "Industrial Security Regulation," February 29, 1984, including Change 1, February 1, 1985, is hereby canceled.

The provisions of this regulation apply to the Office of the Secretary of Defense (OSD), the Organization of the Joint Chiefs of Staff, the Military Departments and the DoD Agencies (hereafter referred to collectively as "DoD Components"), and to other federal agencies. These DoD and Non-DoD Components are collectively referred to as "User Agencies" within this regulation. Send recommended changes to this regulation through channels to:

Director
Defense Investigative Service
ATTN: V0410
1900 Half Street, S.W.
Washington, D.C. 20324-1700

DoD Components may obtain copies of this regulation through their own publication channels. Other federal agencies and the public may obtain copies from the Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, Pennsylvania 19120.

DTIC
ELECTE
S JAN 06 1994
A

Thomas J. O'Brien
THOMAS J. O'BRIEN
Director

DTIC QUALITY INSPECTED 8

This document has been approved
for public release and sale; its
distribution is unlimited

| | |
|--------------------|---|
| Accession For | |
| NTIS | CRA&I <input checked="" type="checkbox"/> |
| DTIC | TAB <input type="checkbox"/> |
| Unannounced | <input type="checkbox"/> |
| Justification | |
| By | |
| Distribution / | |
| Availability Codes | |
| Dist | Avail and/or Spec Di |
| A-1 | |

SECTION I. GENERAL PROVISIONS

Part 1. INTRODUCTION

1-100 Objective. The security of the U.S. 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 U.S. industrial organizations, educational institutions, and all organizations and facilities used by prime and sub-contractors, hereinafter referred to as industry. The objective of this regulation is to set 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 ISM, as a companion document to this regulation, is a DoD publication which contains detailed security requirements to be followed by U.S. contractors for safeguarding classified information. The ISM is made applicable to industry by execution of the "DoD Security Agreement" (DD Form 441), and by direct reference in the "Security Requirements Clause" in the contract. Should * there develop any conflict in instructions between the ISM and this regulation, such conflict shall be reported to the Director, Defense Investigative Service (DIS), ATTN: Deputy Director (Industrial Security). Pending resolution, the provisions of this regulation shall govern.

1-101 Authority and Scope. This regulation, authorized by the Secretary of Defense under the authority of the National Security Act of 1947, as amended, is established as a DoD regulation published by Headquarters (HQ) DIS under the authority of DoD Directive 5220.22, "DoD Industrial Security Program."

a. This regulation is applicable to the OSD (including all of its boards, councils, staffs, and commands), DoD agencies, and the Departments of the Army, Navy, and Air Force (including all of their activities), hereinafter referred to as User Agencies (UA's), in all industrial security relationships with industry.

b. The Secretary of Defense is authorized to act on behalf of the UA's listed in paragraph 1-273.

c. The DIS shall administer the DoD Industrial Security Program on behalf of all UA's.

(1) The Regional Directors of DIS have the authority and responsibility for administration of the DoD Industrial Security Program within their respective regions. The offices of the Directors of Industrial Security are designated as the cognizant security offices (CSO's) for all contractor facilities within their jurisdictions and are responsible for the performance of CSO functions prescribed in this regulation, except for certain security actions noted elsewhere herein which may be performed by the Commander or Head of a UA installation or the Regional Directors of DIS. Facility security clearances (FCL's) shall be granted by the CSO.

(2) The Director, Defense Industrial Security Clearance Office (DISCO), DIS, Columbus, Ohio 43216, shall assume responsibility for processing and granting all industrial personnel security clearances (PCL's) (except for contractor-granted CONFIDENTIAL clearances), including those PCL's for contractor personnel located on a UA installation, and for maintaining an industrial personnel security clearance file (PSCF) of PCL's and FCL's.

(3) UA's have the authority and exercise the functions of, a contracting activity as prescribed in this regulation and the ISM. Certain of these functions, under the delegation of the PCO are performed by the ACO (see appendix C).

d. This regulation implements the security policies established by the Deputy Under Secretary of Defense for Policy (DUSD(P)) and establishes the procedures, requirements, and practices concerned with the effective protection of classified information in the hands of industry, including foreign classified information which the U.S. Government is obliged to protect, in the interest of national security. UA's are not authorized to require a different standard of industrial security than prescribed herein, except as authorized in paragraph 1-114. In addition, this regulation implements the DoD Operations Security (OPSEC) Program established by DUSD(P) as set forth in DoD Directive 5205.2, "DoD Operations Security Program." Section X of this regulation provides amplifying and procedural guidance for UA's when considering imposition of OPSEC requirements on industry. *

(1) This regulation is written in terms of the most common situation where the contractor has access to, or possession of, classified information in connection with the performance of a classified contract. However, it is also applicable to the safeguarding of classified information in connection with all aspects of precontract activity, including preparation of bids and proposals and precontract negotiations, and all aspects of postcontract activity. Moreover, the requirements are equally applicable to the safeguarding of classified information not released or disclosed under a procurement contract such as U. Government-sponsored independent research and development advance agreements. UA programs participated in by a firm, organization, or individual on a voluntary or grant basis. Examples of the latter programs are long-range scientific and technical planning programs and programs designed to provide planning briefings for industry. Contractors participating in such programs shall be advised of the following: "The recipient shall safeguard all classified material and shall provide and maintain a system of security controls within its organization in accordance with the requirements of: (i) the 'Department of Defense Security Agreement' (DD Form 441), (ii) the ISM (attachment to DD Form 441), and (iii) any revisions or changes to the ISM required by the demands of national security as determined by the U.S. Government." In such situations, the official of the UA, or designee, who releases or discloses the classified information to the firm, organization, or individual shall fulfill the responsibilities which this regulation and the ISM assign to the contracting officer (such as, furnishing necessary classification guidance, authorizing retention of classified material, and certifying contractors' need to attend classified meetings).

(2) When foreign classified information is made available to a contractor by a UA in connection with a U.S. classified contract, procedures applicable to U.S. classified information shall be used. However, when foreign classified information is made available to U.S. contractors in connection with a foreign classified contract, the responsibility for the actions which this regulation and the ISM charge to the contracting officer and the contracting UA shall be as prescribed in paragraph 8-103e. Responsibilities not specifically

SUMMARY OF CHANGES

The following is a brief description of substantial changes to the Industrial Security Regulation since February 29, 1984. These changes are marked by an asterisk in the right hand margin of the text. Some paragraphs contain only editorial revisions and therefore are not enumerated.

| | |
|---|--|
| 1-101d, 1-252a, 1-252b, 4-103h, 10-100, 10-101, 10-102, 10-103, and 10-104 | Adds definition, requirements, and guidance concerning OPSEC. |
| 1-103d(5) | Changes DISCO notification responsibilities. |
| 1-108b(13) and 1-108e(7) | Clarifies that if no COMSEC account is required, only FSO must be briefed and debriefed. |
| 1-110a(2), 1-110b thru g, 1-111b, 1-111.1, 1-409, 2-118j and Appendix B (page 224) | Clearance and classified storage verification has been centralized at the Personnel Investigations Center - Central Verifications Activity (PIC-CVA). There are some exceptions. |
| 1-113 | Provides review procedures for unclassified informa- tion processed for public dissemination. |
| 1-114 | Paragraph retitled. Subpara- graph f added to include "carve-out" contracts. |
| 1-205.1 | Adds definition of "carve-out." |
| 1-221.2 | Adds definition of critical technology. |
| 1-227.1 | Adds definition of Essential Elements of Friendly Informa- tion (EEFI). |
| 1-228 | Expands definition of Executive Personnel. |

1-273, 2-309a and
4-201b

Adds United States Information Agency as new UA. Deletes Health and Human Services as UA.

1-304 and 1-407

Revises footnote to include countries whose policies are inimical to U.S. Interests. Changes the term "Communist" countries to "Designated" countries.

1-600, 1-601d and e

Revises procedures for transmission of classified material aboard commercial passenger aircraft. Deletes paragraphs 1-601d and e.

2-106

Adds that a Type A Consultant to a temporary help supplier is prohibited unless used solely by the temporary help supplier.

2-116j(3)

Provides procedures for release of classified material to facilities with Reciprocal FCL's.

2-119

Administrative termination of facility security clearances reduced from 18 months to 9 months.

2-309a(1)(d), and
2-309a(3)

Adds National Guard personnel.

2-309d

Adds new paragraph concerning investigations and clearances by government agencies.

3-103e

Restricts Category 5 visits to U.S. citizens.

3-104

Deletes immigrant aliens. Deletes interim visit approvals.

8-102g(2)(a)

Revised to conform with ISM changes.

8-103e

Adds lead-in paragraph for Table 1 concerning foreign classified contracts responsibilities.

8-302 and Appendix B
(page 225)

Adds OISI Field Office,
Mannheim, West Germany, and
Industrial Security - Far East
office.

A-103c(2) and 1-104

Adds addresses of Military
Department Investigative
Agencies. Provides new
information concerning
Communist personnel stationed
in the U.S.

Appendix E

Adds MTMC emergency hot line
telephone number.

REFERENCES

- (a) DoD 5220.22-M. "Industrial Security Manual for Safeguarding Classified Information," December 2, 1985 authorized by DoD Directive 5220.22, "DoD Industrial Security Program," December 8, 1980 *
- (b) DoD 5220.22-C, "Carrier Supplement to Industrial Security Manual for Safeguarding Classified Information," April 1970, with Change 1, March 15, 1971
- (c) DoD Supplement to the FAR (Reference gg) *
- (d) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 2, 1982
- (e) Reserved
- (f) Reserved
- (g) Public Law 81-11, Section (§) 63 Statute 7, "Export Control Act of 1949"
- (h) Public Law 83-665, § 68 Statute 832, "Mutual Security Act of 1949"
- (i) Title 22, Code of Federal Regulations, Parts 121-128, the same information is contained in "International Traffic in Arms Regulation" (ITAR), published as a brochure by the Department of State
- (j) Reserved
- (k) Reserved
- (l) DoD 5400.7-R, "DoD Freedom of Information Act Program," March 24, 1980
- (m) DoD 5400.11-R, "Department of Defense Privacy Program," June 9, 1982
- (n) Title 8, United States Code (U.S.C.) § 1101(a)(22)
- (o) Public Law 83-703, §§ 11, 68 Statute 919, 924, "Atomic Energy Act of 1954"
- (p) Title 48, United States Code (U.S.C.), § 1681 *
- (q) DoD 5220.22-S-1, "COMSEC Supplement to Industrial Security Manual for Safeguarding Classified Information," August 1983
- (r) National Disclosure Policy (NDP-1), September 9, 1981
- (s) Public Law 91-184, § 83 Statute 841, "Export Administration Act of 1969"
- (t) Public Law 9-629, § 82 Statute 1320 on the Arms Export Control Act (1968)
- (u) National Communications Security Committee Publication NCSC 2, "National Policy on Release of Communications Security Information to U.S. Contractors and Other Nongovernmental Sources"
- (v) Reserved
- (w) Executive Order 12356, "National Security Information," April 2, 1982
- (x) Reserved
- (y) Joint Regulation AR55-355, NAVSUP Instruction 4500.70 (Revised), AFM-72-2, MCO P4600.14 A, DLAR 4500.3, "Military Traffic Management Regulation," March 15, 1969
- (z) Reserved
- (aa) Reserved
- (bb) Reserved
- (cc) Reserved
- (dd) DIS Form 1149, "Department of Defense Transportation Security Agreement," May 1983
- (ee) Public Law 81-774, § 64 Statute 798, "Defense Production Act of 1950"
- (ff) Public Law 85-536, "Small Business Act"

- (gg) Federal Acquisition Regulation
- (hh) DoD Instruction 5200.21, "Dissemination of DoD Technical Information," September 27, 1979
- (ii) Reserved
- (jj) Reserved
- (kk) Public Law 82-414, § 66 Statute 163, "Immigration and Nationality Act of 1952"
- (ll) DoD Directive 5220.6, "Defense Industrial Personnel Security Clearance Review Program," August 12, 1985 *
- (mm) DoD Directive 5200.2, "DoD Personnel Security Program," December 20, 1979 *
- (nn) Title 18, U.S.C., §§ 793, 794, and 798
- (oo) Director of Central Intelligence Directive No. 1/7, "Control and Dissemination of Intelligence Information," May 4, 1981, Implemented within the DoD by DoD Instruction 5230.22, April 1, 1982
- (pp) DoD Directive 5210.41, "Security Criteria and Standards for Protecting Nuclear Weapons," September 12, 1978
- (qq) DoD Directive 5210.42, "Nuclear Weapon Personnel Reliability Program," April 23, 1981
- (rr) DoD 5200.2-R, "DoD Personnel Security Program," December 20, 1979, authorized by DoD Directive 5200.2, "DoD Personnel Security Program," December 20, 1979
- (ss) DLAM 5205.1, "Correspondence," March 30, 1981
- (tt) Reserved
- (uu) Reserved
- (vv) Title 18, U.S. C. 537, Chapter 37
- (ww) Public Law 81-831, § 64 Statute 987, 989, 991, and 992, Chapter 1024, "Subversive Activities Control Act of 1950"
- (xx) DoD Instruction 5240.4, "Reporting of Counterintelligence and Criminal Violations," July 28, 1983 *
- (yy) DoD 5200.1-R, "Information Security Program Regulation," July 12, 1982, authorized by DoD Directive 5200.1, "DoD Information Security Program," June 7, 1982 *
- (zz) DoD Directive 5100.36, "Defense Scientific and Technical Information Program," October 2, 1981
- (aaa) DIS 31-4-R "Industrial Security Operating Regulation" (ISOR), September 4, 1984
- (bbb) DoD 5000.12-M, "DoD Directive Manual for Standard Data Elements," December 1981, authorized by DoD Directive 5000.12, "Data Elements and Data Codes Standardization Procedures," April 27, 1965
- (ccc) Public Law 77-831, § 56 Statute 1078, "Federal Reports Act of 1942"
- (ddd) Public Law 75-583, § 52 Statute, "Foreign Agent Registration Act of 1938," as amended in Public Law 77-532, § 56 Statute 248 (1942)
- (eee) JCS Pub 1, "Department of Defense Dictionary of Military and Associated Terms," June 1, 1979

GLOSSARY OF ACRONYMS AND ABBREVIATIONS COMMONLY USED IN THE DOD INDUSTRIAL SECURITY PROGRAM

| | | |
|--------------------|---|---|
| ACO | Administrative Contracting Officer | |
| ACDA | U.S. Arms Control and Disarmament Agency | |
| ACSI | Assistant Chief of Staff for Intelligence, Department of Army | |
| ADP | Automatic Data Processing | |
| APO | Army Post Office | |
| ARFCOS | Armed Forces Courier Service | |
| ASD(C) | Assistant Secretary of Defense (Comptroller) | |
| BI | Background Investigation | |
| BL | Bill of Lading | |
| (C) | CONFIDENTIAL | |
| CAB | Civil Aeronautics Board | |
| CAGE | Commercial and Government Entity Number (formerly FSC) | * |
| CBL | Commercial Bill(s) of Lading | |
| CDSS | Canadian Department of Supply and Services | |
| CENTO | Central Treaty Organization | |
| CM | Candidate Material | |
| CNWDI | Critical Nuclear Weapon Design Information | |
| COMINT | Communications Intelligence | |
| COMSEC | Communications Security | |
| CONUS | Continental United States | |
| COR | Central Office of Record | |
| COSMIC-TOP | | |
| SECRET | Property of NATO and Subject to Special Security Controls | |
| CSISM | COMSEC Supplement to the Industrial Security Manual | |
| CSO | Cognizant Security Office | |
| CVA | Central Verifications Activity | * |
| DCASR | Defense Contract Administration Services Region | |
| DCII | Defense Central Index of Investigations | |
| DGSC | Defense General Supply Center | * |
| DIA | Defense Intelligence Agency | |
| DIS | Defense Investigative Service | |
| DISCO | Defense Industrial Security Clearance Office | |
| DISCR, OGC, OSD | Director for Industrial Security Clearance Review, Office of the General Counsel, Office of Secretary of Defense | |
| DSI | Defense Security Institute | * |
| DLA | Defense Logistics Agency | |
| DNACC | Defense National Agency Check Center | |
| DoD | Department of Defense | |
| DoDAAD | Department of Defense Activity Address Directory | |
| DOE | Department of Energy (formerly ERDA) | |
| DOIS | Director, Office of Industrial Security | |
| DOJ | Department of Justice | |
| DOT | Department of Transportation | |
| DSP&P | Director for Security Plans & Programs, Office of the Deputy Under Secretary of Defense for Policy Review | |
| DTIC | Defense Technical Information Center | |

| | | |
|---------|---|---|
| DUSD | Deputy Under Secretary of Defense | |
| DUSD(P) | Deputy Under Secretary of Defense for Policy | * |
| EEFI | Essential Elements of Friendly Information | * |
| ENAC | Expanded National Agency Check | |
| E.O. | Executive Order | |
| EPA | Environmental Protection Agency | |
| FAA | Federal Aviation Agency (presently Federal Aviation Administration, Department of Transportation) | |
| FAR | Federal Acquisition Regulation | |
| FBI | Federal Bureau of Investigation | |
| FCL | Facility Security Clearance | |
| FEMA | Federal Emergency Management Agency | |
| FMS | Foreign Military Sales | |
| FOCI | Foreign Ownership, Control, or Influence | |
| (FRD) | FORMERLY RESTRICTED DATA | |
| FRS | Federal Reserve System | |
| FSC | Federal Supply Code (see CAGE) | * |
| FSO | Facility Security Supervisor/Officer | |
| FSS | Federal Supply Schedule | |
| GAO | General Accounting Office | |
| GBL | Government Bill(s) of Lading | |
| GFE | Government Furnished Equipment | |
| GFP | Government Furnished Property | |
| GPO | Government Printing Office | |
| GSA | General Services Administration | |
| GSOIA | General Security of Information Agreement | |
| HOF | Home Office Facility | |
| HQ | Headquarters | |
| ICC | Interstate Commerce Commission | |
| IFB | Invitation for Bid | |
| INSCOM | Intelligence and Security Command | * |
| IPO | International Pact Organization | |
| ISB | Industrial Security Bulletin | |
| ISL | Industrial Security Letter | |
| ISM | "Industrial Security Manual for Safeguarding Classified Information" (DoD 5220.22-M) | |
| ISR | "Industrial Security Regulation" (DoD 5220.22-R) | |
| ITAR | "International Traffic in Arms Regulations" | |
| KGB | Committee on State Security (Soviet Union) | |
| LOC | Letter of Consent (DISCO Form 560) | |
| MAAG | Military Assistance Advisory Group | |
| MAP | Mutual Aid Program | |
| MDAP | Mutual Defense Assistance Program | |
| MFO | Multiple Facility Organization | |
| MIL-STD | Military Standard (Book Form) | |
| MMMC | Military Traffic Management Command (formerly MTMTS) | |

| | | |
|----------|---|---|
| N/A | Not Applicable | |
| NAC | National Agency Check | |
| NASA | National Aeronautics and Space Administration | |
| NATO | North Atlantic Treaty Organization | |
| NCSC | National Communications Security Committee | |
| NIS | Naval Investigative Service | |
| NPLO | NATO Production Logistics Organization | |
| NRC | Nuclear Regulatory Commission | |
| NSA | National Security Agency | |
| NSF | National Science Foundation | |
| | | |
| OASD(C) | Office of the Assistant Secretary of Defense (Comptroller) | |
| OASD(PA) | Office of the Assistant Secretary of Defense (Public Affairs) | |
| OGC | Office of General Counsel | |
| OISI | Office of Industrial Security International | |
| OODEPs | Owners, Officers, Directors, Partners, Regents, Trustees, or Executive Personnel | |
| OPSEC | Operations Security | * |
| OSD | Office of Secretary of Defense | |
| OSI | Office of Special Investigations, USAF | |
| | | |
| PCO | Procuring Contracting Officer | |
| PCL | Personnel Security Clearance | |
| PIC | Personnel Investigations Center | * |
| PMF | Principal Management Facility | |
| PRP | Personnel Reliability Program | |
| PSCF | Industrial Personnel Security Clearance Files (formerly CIF) | |
| PSQ | Personnel Security Questionnaire | |
| PSS | Protective Security Service | |
| | | |
| (RD) | RESTRICTED DATA | |
| RFI | Representative of a Foreign Interest | |
| RFP | Request for Proposal | |
| RFQ | Request for Quote | |
| | | |
| (S) | SECRET | |
| SBA | Small Business Administration | |
| SCI | Sensitive Compartmented Information | |
| SEATO | Southeast Asia Treaty Organization | |
| SIOP | Single Integrated Operational Plan | |
| SPP | Standard Practice Procedure(s) | |
| SSS | Signature Security Service | |
| | | |
| TO | Transportation Officer | |
| (TS) | TOP SECRET | |
| TSEC | U.S. Telecommunications Security | |
| TWX | Teletype Communications | |
| | | |
| (U) | UNCLASSIFIED | |
| UA | User Agency | |
| U.K. | United Kingdom | |
| UL | Underwriters' Laboratories | |
| U.S. | United States | |
| USAFSS | U.S. Air Force Security Service | |

| | |
|-------------|--|
| USASTRATCOM | U.S. Army Strategic Communications Command |
| U.S.C | United States Code |
| USIA | U.S. Information Agency |
| USIB | U.S. Intelligence Board |

TABLE OF CONTENTS

| <u>Paragraph</u> | <u>Page</u> |
|---|-------------|
| Foreward | i |
| Summary of Changes | iii |
| References | v |
| Glossary of Acronyms and Abbreviations Commonly Used in the DoD Industrial Security Program. | vii |

Section I. GENERAL PROVISIONS

Part 1. INTRODUCTION

| | | | |
|---------|--|----|---|
| 1-100 | Objective | 1 | |
| 1-101 | Authority and Scope | 1 | |
| 1-102 | Superseded Regulation | 3 | |
| 1-103 | Responsibilities | 3 | |
| 1-104 | Arrangement of Regulation | 5 | |
| 1-105 | Amendment of Regulation | 5 | |
| 1-106 | Distribution and Use of Regulation | 5 | |
| 1-107 | User Agency Procedures Under this Regulation | 6 | |
| 1-108 | Contractor Activities on a User Agency Installation | 6 | |
| 1-109 | Expenditure of Funds for Security | 9 | |
| 1-110 | Disclosure of Classified Information to a Contractor by User Agency Contracting Activities | 9 | |
| 1-111 | Disclosure of Classified Information to a Subcontractor by a Prime Contractor | 12 | |
| 1-111.1 | Disclosure of Critical Nuclear Weapon Design Information (CNWDI). | 13 | |
| 1-112 | Applicability to Subcontractors and Their Employees | 13 | |
| 1-113 | Public Disclosure | 13 | * |
| 1-114 | Waivers, Special Access Programs, and Carve-outs | 15 | * |
| 1-115 | Security Administration of U.S. Classified Contracts Awarded to U.S. Contractors for Performance Abroad | 16 | |
| 1-116 | Privileged Information | 17 | |

Part 2. DEFINITION OF TERMS

| | | | |
|---------|---|----|---|
| 1-200 | Definitions | 18 | |
| 1-201 | Access, Accessibility | 18 | |
| 1-202 | Accountable COMSEC Material | 18 | |
| 1-203 | Alien | 19 | |
| 1-204 | Authorized Persons | 19 | |
| 1-205 | Candidate Material | 19 | |
| 1-205.1 | Carve-out | 19 | * |
| 1-206 | Central Office of Record (COR). | 19 | |

| | | |
|---------|---|-----|
| 1-207 | Channels for the Dissemination of COMSEC Material | 19 |
| 1-208 | Classified Contract | 19 |
| 1-208.1 | Classification Guide | 19 |
| 1-209 | Classified Information | 19 |
| 1-209.1 | Classifier | 20 |
| 1-210 | Closed Area | 20 |
| 1-211 | Cognizant Security Office (CSO) | 20 |
| 1-212 | Colleges and Universities | 20 |
| 1-213 | Reserved | 20 |
| 1-214 | Communications Intelligence | 20 |
| 1-215 | Communications Security (COMSEC) | 20 |
| 1-216 | Communications Security (COMSEC) Information | 20 |
| 1-217 | Compromise | 20 |
| 1-217.1 | Compromising Emanations | 20 |
| 1-218 | CONFIDENTIAL | 21 |
| 1-219 | Continental Limits of the United States | 21 |
| 1-220 | Contracting Officer | 21 |
| 1-221 | Contractor | 21 |
| 1-221.1 | CNWDI | 21 |
| 1-221.2 | Critical Technology | 21 |
| 1-222 | CRYPTO | 22 |
| 1-223 | CRYPTOSYSTEM | 22 |
| 1-223.1 | Custodian | 22 |
| 1-224 | Declassification | 22 |
| 1-225 | Department of Defense | 22 |
| 1-225.1 | Derivative Classification | 22 |
| 1-226 | Document | 22 |
| 1-227 | Downgrade | 22 |
| 1-227.1 | Essential Elements of Friendly Information | 22 |
| 1-228 | Executive Personnel | 23 |
| 1-229 | Facility | 23 |
| 1-230 | Facility Security Clearance (FCL) | 23 |
| 1-231 | Foreign Government Information | 23 |
| 1-231.1 | Foreign Interest | 23 |
| 1-232 | Foreign Nationals | 23 |
| 1-233 | FORMERLY RESTRICTED DATA | 23 |
| 1-234 | Graphic Arts | 24 |
| 1-235 | Handling | 24 |
| 1-236 | Home Office (HOF) | 24 |
| 1-237 | Immigrant Alien | 24 |
| 1-238 | Industrial Security | 24 |
| 1-239 | Information Security | 24 |
| 1-240 | Intelligence | 24 |
| 1-241 | Interim Security Clearance | 24 |
| 1-242 | Internal Security | 24 |
| 1-243 | Locked Entrance | 24 |
| 1-244 | Long Title | 24 |
| 1-245 | Material | 24 |
| 1-246 | Multiple Facility Organization (MFO) | 24a |
| 1-247 | National of the United States | 24a |
| 1-248 | NATO Classified Information | 24a |
| 1-249 | Need-To-Know | 24a |
| 1-250 | Negotiator | 24a |
| 1-251 | Officers (Corporation, Association, or Other Types of Business or Educational Institution) | 24a |

| | | | |
|---------|---|-----|---|
| 1-252 | Official Information | 24a | |
| 1-252a | Operations Security (OPSEC) | 24b | * |
| 1-252b | OPSEC Indicators | 24b | * |
| 1-252.1 | Parent | 24b | |
| 1-253 | Possessions | 24b | |
| 1-253.1 | Principal Management Facility (PMF) | 24b | |
| 1-254 | Reference Material | 24b | |
| 1-255 | Regrade | 24b | |
| 1-256 | Representatives of a Foreign Interest (RFI's) | 24b | |
| 1-257 | Restricted Area | 24c | |
| 1-258 | RESTRICTED DATA | 24c | |
| 1-259 | SECRET | 24c | |
| 1-260 | Security | 24c | |
| 1-261 | Security Cognizance | 24c | |
| 1-261.1 | SENSITIVE COMPARTMENTED INFORMATION | 24c | |
| 1-262 | Short Title | 25 | |
| 1-263 | Special Access Program | 25 | |
| 1-264 | Subsidiary | 25 | |
| 1-265 | Telecommunications | 25 | |
| 1-265.1 | TEMPEST | 25 | |
| 1-266 | Time Resource Sharing | 25 | |
| 1-267 | TOP SECRET | 25 | |
| 1-268 | Transmission Security | 25 | |
| 1-269 | Trust Territory | 25 | |
| 1-270 | Unauthorized Person | 26 | |
| 1-271 | United States | 26 | |
| 1-272 | Upgrade | 26 | |
| 1-273 | User Agencies (UA's) | 26 | |

Part 3. SECURITY COGNIZANCE

| | | |
|-------|---|----|
| 1-300 | Policy | 26 |
| 1-301 | Functions of a Cognizant Security Office | 27 |
| 1-302 | Notification of Security Assignment | 27 |
| 1-303 | Procedural Changes | 27 |
| 1-304 | Defensive Security Briefing | 28 |
| 1-305 | Responsibility for the Security of SENSITIVE COMPARTMENTED INFORMATION Contracts | 29 |
| 1-306 | Operational Responsibility for NSA COMSEC Account | 30 |

Part 4. SPONSORSHIP OF MEETINGS

| | | |
|-------|--|----|
| 1-400 | Application | 30 |
| 1-401 | General Policy | 30 |
| 1-402 | Requests for Sponsorship | 31 |
| 1-403 | Guides for Sponsorship | 31 |
| 1-404 | Location of Meetings | 32 |
| 1-405 | Security Procedures | 32 |
| 1-406 | Controlling Disclosures | 34 |
| 1-407 | Attendance by Foreign Nationals and Representatives of a Foreign Interest | 34 |
| 1-408 | Disclosure Authorizations | 35 |
| 1-409 | Approval for Attendance at Classified Meetings | 35 |
| 1-410 | Notification | 36 |

Part 5. PROCEDURES PERTAINING TO COMSEC INFORMATION

| | | |
|-------|---|----|
| 1-500 | Application | 36 |
| 1-501 | Instructions Concerning COMSEC Material | 36 |
| 1-502 | Release of COMSEC Information and Material to U.S. Contractors | 37 |
| 1-503 | Subcontracting COMSEC Work | 38 |
| 1-504 | Establishing a COMSEC Account | 38 |
| 1-505 | Destruction and Disposition of COMSEC Material | 39 |
| 1-506 | Shipment of COMSEC Material Outside of a Facility | 39 |
| 1-507 | Unsolicited COMSEC Proposals | 39 |

Part 6. TRANSMISSION OF CLASSIFIED MATERIAL

| | | |
|-------|--|----|
| 1-600 | Application | 39 |
| 1-601 | Approved Methods of Transmission | 39 |
| 1-602 | Contracting Officer Approval | 40 |
| 1-603 | NATO Hand-carried Material. | 41 |

Part 7. PROCEDURES PERTAINING TO COMMERCIAL CARRIERS

| | | |
|-------|--|----|
| 1-700 | Application | 42 |
| 1-701 | Instructions Concerning Commercial Carriers | 42 |
| 1-702 | Approval of Commercial Carriers | 42 |
| 1-703 | Responsibilities of Cognizant Security Offices | 44 |

Section II. CLEARANCE PROCEDURES**Part 1. FACILITY SECURITY CLEARANCES AND DENIALS**

| | | |
|-------|--|----|
| 2-100 | Application | 47 |
| 2-101 | Eligibility for Access | 47 |
| 2-102 | Facility Security Clearances | 47 |
| 2-103 | Responsibility for Effecting a Facility Security Clearance | 48 |
| 2-104 | Types of Facilities | 48 |
| 2-105 | Consultants — General Requirements | 52 |
| 2-106 | Consultants, Type A | 52 |
| 2-107 | Consultants, Type B | 53 |
| 2-108 | Consultants, Type C | 53 |
| 2-109 | Consultants to User Agencies Employed Under Civil Service Procedures | 54 |
| 2-110 | National Agency Check (NAC)(Facility) | 54 |
| 2-111 | Requirements for Facility Security Clearances and Annual Review | 55 |
| 2-112 | RESTRICTED DATA, Additional Facility Security Clearance Requirements | 57 |
| 2-113 | Personnel Required to be Cleared for a Facility Security Clearance | 57 |
| 2-114 | Foreign Nationals Serving as Officers, Partners or Members of Boards of Directors | 63 |
| 2-115 | Clearance of Negotiators | 64 |

| | | | |
|-------|---|----|---|
| 2-116 | Procedures for Processing a Facility Security Clearance | 64 | |
| 2-117 | Facility Security Assurances | 70 | * |
| 2-118 | Changed Conditions Pertaining to the Facility | 71 | |
| 2-119 | Administrative Termination of a Facility Security Clearance | 76 | |
| 2-120 | Reprocessing or Revalidating a Facility Security Clearance | 77 | |
| 2-121 | Denial, Suspension, or Revocation of a Facility Security Clearance | 78 | |
| 2-122 | Appeals Not Authorized | 81 | |
| 2-123 | Reprocessing of a Facility Security Clearance That Has Been Revoked | 81 | |

Part 2. U.S. FACILITIES THAT ARE FOREIGN OWNED, CONTROLLED, OR INFLUENCED

| | | |
|-------|---|----|
| 2-200 | Application | 81 |
| 2-201 | General Policy | 82 |
| 2-202 | Factors | 82 |
| 2-203 | Procedures | 83 |
| 2-204 | Assistance | 84 |
| 2-205 | Methods to Negate or Reduce Risk in Foreign Ownership Cases | 85 |
| 2-206 | Visitation Agreements | 89 |
| 2-207 | Certification and Compliance | 89 |
| 2-208 | Effects of this Part on Prior Facility Security Clearances | 89 |

Part 3. PERSONNEL SECURITY CLEARANCES AND DENIALS FOR CONTRACTOR PERSONNEL

| | | |
|-------|---|------|
| 2-300 | Application | 90 |
| 2-301 | Security Clearances for Personnel | 90 |
| 2-302 | Defense Industrial Security Clearance Office | 92 |
| 2-303 | Special Status of Certain American Indians Born in Canada | 93 |
| 2-304 | Transfer of Personnel Between Facilities of a Multiple Facility Organization | 93 |
| 2-305 | Processing of a Hostage Case | 93 |
| 2-306 | Processing of a Representative of a Foreign Interest Case | 94 |
| 2-307 | Responsibility for Effecting Contractor Personnel Security Clearances | 96 |
| 2-308 | Requirements for Security Clearances for Contractor Personnel | 98 |
| 2-309 | Conversion of Clearances for Civilian and Military Personnel of the Department of Defense and Certain Other Governmental Agencies | 101 |
| 2-310 | Administrative Termination of Personnel Security Clearances | 105a |

| | | |
|---------|---|-----|
| 2-311 | Administrative Downgrading of TOP SECRET | |
| | Personnel Security Clearances. | 107 |
| 2-312 | RESTRICTED DATA, Additional Clearance Requirements | 107 |
| 2-312.1 | Requirements for Access to CNWDI | 108 |
| 2-313 | Requirements for Access to Classified COMSEC Information. | 108 |
| 2-314 | COMSEC Briefing and Debriefing Requirements | 109 |
| 2-315 | Additional Requirements for SENSITIVE | |
| | COMPARTMENTED INFORMATION Material | 110 |
| 2-316 | Denial of Admittance to User Agency Installations | 110 |
| 2-317 | Intelligence Briefing and Debriefing Requirements | 110 |
| 2-318 | CONFIDENTIAL Security Clearances for Personnel of | |
| | Colleges and Universities. | 111 |
| 2-319 | Types of Personnel Investigations | 111 |
| 2-319.1 | User Agency Responsibility to Report Adverse Information. | 112 |
| 2-320 | Denial, Suspension, or Revocation of Personnel | |
| | Security Clearances. | 112 |
| 2-321 | Access to NATO Classified Information | 114 |
| 2-322 | U.S. Security Assurances for U.S. Citizens Under Bilateral | |
| | Reciprocal Security Agreements | 114 |
| 2-323 | Security Assurances for Nationals of Signatory | |
| | Governments Under Bilateral Reciprocal | |
| | Industrial Security Agreements | 114 |
| 2-324 | Requirements of the Nuclear Weapon Personnel | |
| | Reliability Program (PRP). | 114 |
| 2-325 | Reserved. | 115 |
| 2-326 | Reserved. | 115 |
| 2-327 | Immigrant Alien Clearance for Access to SECRET | |
| | and CONFIDENTIAL Information | 115 |

Part 4. MAINTENANCE OF FACILITY FILES AND DISCO RECORDS

| | | |
|-------|---|-----|
| 2-400 | Application | 115 |
| 2-401 | Maintenance of Facility Folders | 115 |
| 2-402 | Responsibilities of the Cognizant Security Office | 116 |
| 2-403 | Responsibilities of DISCO | 117 |
| 2-404 | Use of Information. | 117 |

Section III. VISITORS

Part 1. VISITS TO USER AGENCY CONTRACTORS

| | | |
|-------|---|-----|
| 3-100 | Application | 119 |
| 3-101 | General | 119 |
| 3-102 | Long-Term Visits. | 120 |
| 3-103 | Visitor Categories and Procedures | 120 |
| 3-104 | Investigative Requirements. | 124 |
| 3-105 | RESTRICTED DATA | 124 |
| 3-106 | East-West Visit Exchange Program. | 125 |

Part 2. VISITS TO USER AGENCY ACTIVITIES

| | | |
|-------|--|-----|
| 3-200 | Application | 125 |
| 3-201 | General Rules | 125 |
| 3-202 | Visits to User Agency Activities in the United States . . . | 126 |
| 3-203 | Visits to User Agency Activities Outside the United States. | 127 |
| 3-204 | Action by Commander or Head of Activity to be Visited . . . | 127 |
| 3-205 | Compliance with Request from the Commander or Head of the User Agency Activity. | 128 |

Part 3. VISITS TO GOVERNMENT ACTIVITIES OTHER THAN USER AGENCIES

| | | |
|-------|---|-----|
| 3-300 | Application | 128 |
| 3-301 | Visits to DOE Installations or DOE Contractors. | 128 |
| 3-302 | Visits to Activities Other Than the Department of Energy. . | 129 |

Part 4. VISITS TO FOREIGN GOVERNMENTS AND ACTIVITIES

| | | |
|-------|-----------------------|-----|
| 3-400 | Application | 129 |
| 3-401 | Use of OISI | 131 |

Part 5. VISITS IN CONNECTION WITH BILATERAL INDUSTRIAL SECURITY AGREEMENTS AND NATO VISIT PROCEDURES

| | | |
|-------|---|-----|
| 3-500 | Visits in Connection with Bilateral Industrial Security Agreements | 131 |
| 3-501 | NATO Visit Procedures | 132 |
| 3-502 | NATO Production Logistics Organization (NPLO) Program Security Clearance and Visit Procedures. | 133 |
| 3-503 | Certificate of Security Clearance | 134 |

Section IV. SECURITY INSPECTIONS

Part 1. INSPECTIONS

| | | |
|---------|--|-----|
| 4-100 | Application | 137 |
| 4-101 | Purpose | 137 |
| 4-102 | Reciprocal Use of DOE and DoD Security Inspection Program . | 137 |
| 4-103 | Schedule. | 139 |
| 4-104 | Notification of Inspection. | 140 |
| 4-105 | Use of Industrial Security Inspection Report (DD Form 696) . | 141 |
| 4-105.1 | TEMPEST Countermeasures | 142 |
| 4-106 | Use of the DIS Form 1148. | 143 |
| 4-107 | COMSEC Inspections. | 143 |
| 4-108 | Formal Notification | 144 |

Part 2. UNSATISFACTORY INSPECTIONS

| | | |
|-------|---|-----|
| 4-200 | Application | 144 |
| 4-201 | Procedures. | 144 |
| 4-202 | Unsatisfactory Evaluation of a Commercial Carrier | 147 |

Part 3. "CLOSE-OUT" INSPECTIONS

| | | |
|-------|-------|-----|
| 4-300 | | 147 |
|-------|-------|-----|

Section V. ESPIONAGE, SABOTAGE, LOSS, COMPROMISE, AND OTHER VIOLATIONS

| | | |
|-------|--|-----|
| 5-100 | Application | 149 |
| 5-101 | Espionage, Sabotage, and Subversive Activities | 149 |
| 5-102 | Loss, Compromise, and Suspected Compromise | 150 |
| 5-103 | Investigative Support | 152 |
| 5-104 | Additional Reporting of Espionage, Criminal Activity, and Deliberate Compromise Cases | 153 |
| 5-105 | Other Security Violations | 154 |
| 5-106 | Other Administrative Violations | 155 |
| 5-107 | Responsibility of Contracting User Agency to Investigate Certain Breaches of Security | 156 |
| 5-108 | Inquiries into Delays, Tampering, or Improper Shipping Methods | 156 |

Section VI. INDUSTRIAL SECURITY EDUCATION

| | | |
|-------|--------------------------------|-----|
| 6-100 | Application | 159 |
| 6-101 | Responsibility | 159 |
| 6-102 | Preparation of Material | 159 |
| 6-103 | Funding | 159 |
| 6-104 | Material Available | 159 |
| 6-105 | Distribution of Material | 160 |
| 6-106 | Training Schools | 160 |

Section VII. SECURITY CLASSIFICATION AND DECLASSIFICATION

| | | |
|-------|--|-----|
| 7-100 | Application | 161 |
| 7-101 | Security Classification | 162 |
| 7-102 | Issuance of Security Classification Guidance | 162 |
| 7-103 | Required Distribution | 168 |
| 7-104 | Review of Classification and Need-to-Know | 169 |
| 7-105 | Classification Interpretation Procedures | 170 |
| 7-106 | Responsibility for Authorizing Retention of Classified Material at Completion of a Contract | 171 |
| 7-107 | Downgrading and Declassification | 173 |
| 7-108 | Protective Marking — FOR OFFICIAL USE ONLY | 173 |

Section VIII. INTERNATIONAL SECURITY PROGRAMS

Part 1. INTERNATIONAL CONTRACTS

| | | |
|-------|-------------------------------------|-----|
| 8-100 | Purpose | 175 |
| 8-101 | Bilateral Security Agreements | 175 |

| | | |
|-------|--|-----|
| 8-102 | General | 176 |
| 8-103 | Foreign Government Classified Contracts or Subcontracts to U.S. Industry | 178 |
| 8-104 | Procedure for the Security of U.S. Classified Contracts or Subcontracts Awarded to a Foreign Contractor | 184 |

**Part 2. PROCEDURES PERTAINING TO U.S. PATENT AGENTS ENGAGED
IN FILING CLASSIFIED PATENT APPLICATIONS FOR FOREIGN GOVERNMENTS**

| | | |
|-------|-----------------------------------|-----|
| 8-200 | Application | 185 |
| 8-201 | General | 185 |
| 8-202 | Procedures | 186 |
| 8-203 | Participating Countries | 187 |

Part 3. OFFICE OF INDUSTRIAL SECURITY, INTERNATIONAL

| | | |
|-------|---------------------|-----|
| 8-300 | General | 187 |
| 8-301 | Functions | 187 |
| 8-302 | Addresses | 187 |

Part 4. OVERSEAS OPERATIONS OF U.S. CONTRACTORS

| | | |
|-------|--|-----|
| 8-400 | General | 188 |
| 8-401 | Access | 188 |
| 8-402 | Safeguarding U.S. Classified Information | 189 |

**Part 5. ACCESS TO CLASSIFIED INFORMATION OF FOREIGN GOVERNMENTS AND
INTERNATIONAL PACT ORGANIZATIONS UNDER A U.S. SECURITY ASSURANCE**

| | | |
|-------|--|-----|
| 8-500 | General | 191 |
| 8-501 | Security Assurances | 191 |
| 8-502 | Administrative Termination of Letters of Consent | 192 |
| 8-503 | Annotation of Clearance Records | 192 |

Section IX. INDUSTRIAL SECURITY FORMS

Part 1. GENERAL

| | | |
|-------|--|-----|
| 9-100 | Application and Index of Forms | 193 |
|-------|--|-----|

Part 2. EXHIBITS OF FORMS

| | | |
|---------|---|-----|
| 9-200 | Purpose | 196 |
| 9-201 | "Facility Security Clearance Survey" (DD Form 374) | 196 |
| 9-202 | "Central Index File Card-Facility" (DIS Form 553) | 199 |
| 9-202.1 | Checklist for the Preparation of DIS Form 553 | 199 |
| 9-203 | "Central Index File Request" (DD Form 555) | 203 |
| 9-203.1 | Checklist for Preparation of DD Form 555. | 203 |
| 9-204 | "Industrial Security Inspection Report" (DD Form 696) | 206 |
| 9-204.1 | Guideline Questions for Industrial Security Inspections (DD Form 696). | 206 |

| | | |
|---------|--|-----|
| 9-204.2 | Explanation of DD Form 696 Items | 206 |
| 9-204.3 | General Note for Personnel Processing This Report | 207 |
| 9-205 | Reserved | 211 |
| 9-206 | "Industrial Security Survey/Inspection Report (Commercial Carrier)" (DIS Form 1148) | 211 |
| 9-206.1 | Instructions for Completing the DIS Form 1148 | 211 |

SECTION X. OPERATIONS SECURITY (OPSEC)

| | | | |
|--------|--|------|---|
| 10-100 | Purpose | 212a | * |
| 10-101 | General | 212a | * |
| 10-102 | Application | 212b | * |
| 10-103 | Responsibilities | 212c | * |
| 10-104 | Procedures for Inspecting OPSEC Programs | 212d | * |

APPENDIX A. RELEASE OF ECONOMIC AND TECHNICAL INFORMATION

| | | |
|-------|--|-----|
| A-100 | Application | 213 |
| A-101 | Release of Economic and Technical Information | 213 |
| A-102 | Replying to Questionnaires | 214 |
| A-103 | Requests From Communist Countries for Unclassified Information of Strategic, Scientific and Technical Intelligence Value | 215 |
| A-104 | Industrial Security and Communist Espionage | 216 |

APPENDIX B. INFORMATION REGARDING COGNIZANT SECURITY OFFICES,
DISCO, DISI, AND OISI

| | |
|---|-----|
| Operational Areas of DIS Cognizant Security Offices | 220 |
| Telephone Numbers and Addresses | 224 |

APPENDIX C. INDUSTRIAL SECURITY FUNCTIONAL RESPONSIBILITIES OF
A CONTRACTING OFFICER

| | |
|---|-----|
| Industrial Security Functional Responsibilities of a Contracting Officer | 227 |
|---|-----|

APPENDIX D. PREPARATION OF CLASSIFICATION GUIDANCE

| | | |
|-------|--|-----|
| D-100 | Application | 231 |
| D-101 | Determining Classification | 231 |
| D-102 | Suggested Method for Development of Guidance | 232 |

APPENDIX E

| | |
|--|-----|
| Areas Serviced by MTMC and by Military Commanders in Alaska, Hawaii, Puerto Rico, and U.S. Possessions and Trust Territories | 235 |
|--|-----|

| | | |
|-------|--|-----|
| E-100 | MTMC | 235 |
| E-101 | Designated Military Commanders | 235 |

APPENDIX F

| | |
|---|-----|
| Functional Responsibilities of MTMC, TO, and CSO. | 237 |
|---|-----|

APPENDIX G

| | |
|---|-----|
| Formats Necessary for NATO Hand-carried Materials | 239 |
|---|-----|

APPENDIX H

| | |
|-----------------|-----|
| Index | 245 |
|-----------------|-----|

SECTION I. GENERAL PROVISIONS**Part 1. INTRODUCTION**

1-100 **Objective.** The security of the U.S. 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 U.S. industrial organizations, educational institutions, and all organizations and facilities used by prime and sub-contractors, hereinafter referred to as industry. The objective of this regulation is to set 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 ISM, as a companion document to this regulation, is a DoD publication which contains detailed security requirements to be followed by U.S. contractors for safeguarding classified information. The ISM is made applicable to industry by execution of the "DoD Security Agreement" (DD Form 441), and by direct reference in the "Security Requirements Clause" in the contract. Should * there develop any conflict in instructions between the ISM and this regulation, such conflict shall be reported to the Director, Defense Investigative Service (DIS), ATTN: Deputy Director (Industrial Security). Pending resolution, the provisions of this regulation shall govern.

1-101 **Authority and Scope.** This regulation, authorized by the Secretary of Defense under the authority of the National Security Act of 1947, as amended, is established as a DoD regulation published by Headquarters (HQ) DIS under the authority of DoD Directive 5220.22, "DoD Industrial Security Program."

a. This regulation is applicable to the OSD (including all of its boards, councils, staffs, and commands), DoD agencies, and the Departments of the Army, Navy, and Air Force (including all of their activities), hereinafter referred to as User Agencies (UA's), in all industrial security relationships with industry.

b. The Secretary of Defense is authorized to act on behalf of the UA's listed in paragraph 1-273.

c. The DIS shall administer the DoD Industrial Security Program on behalf of all UA's.

(1) The Regional Directors of DIS have the authority and responsibility for administration of the DoD Industrial Security Program within their respective regions. The offices of the Directors of Industrial Security are designated as the cognizant security offices (CSO's) for all contractor facilities within their jurisdictions and are responsible for the performance of CSO functions prescribed in this regulation, except for certain security actions noted elsewhere herein which may be performed by the Commander or Head of a UA installation or the Regional Directors of DIS. Facility security clearances (FCL's) shall be granted by the CSO.

(2) The Director, Defense Industrial Security Clearance Office (DISCO), DIS, Columbus, Ohio 43216, shall assume responsibility for processing and granting all industrial personnel security clearances (PCL's) (except for contractor-granted CONFIDENTIAL clearances), including those PCL's for contractor personnel located on a UA installation, and for maintaining an industrial personnel security clearance file (PSCF) of PCL's and FCL's.

(3) UA's have the authority and exercise the functions of, a contracting activity as prescribed in this regulation and the ISM. Certain of these functions, under the delegation of the PCO are performed by the ACO (see appendix C).

d. This regulation implements the security policies established by the Deputy Under Secretary of Defense for Policy (DUSD(P)) and establishes the procedures, requirements, and practices concerned with the effective protection of classified information in the hands of industry, including foreign classified information which the U.S. Government is obliged to protect, in the interest of national security. UA's are not authorized to require a different standard of industrial security than prescribed herein, except as authorized in paragraph 1-114. In addition, this regulation implements the DoD Operations Security (OPSEC) Program established by DUSD(P) as set forth in DoD Directive 5205.2, "DoD Operations Security Program." Section X of this regulation provides amplifying and procedural guidance for UA's when considering imposition of OPSEC requirements on industry. *

(1) This regulation is written in terms of the most common situation where the contractor has access to, or possession of, classified information in connection with the performance of a classified contract. However, it is also applicable to the safeguarding of classified information in connection with all aspects of precontract activity, including preparation of bids and proposals and precontract negotiations, and all aspects of postcontract activity. Moreover, the requirements are equally applicable to the safeguarding of classified information not released or disclosed under a procurement contract such as U.S. Government-sponsored independent research and development advance agreements or UA programs participated in by a firm, organization, or individual on a voluntary or grant basis. Examples of the latter programs are long-range scientific and technical planning programs and programs designed to provide planning briefings for industry. Contractors participating in such programs shall be advised of the following: "The recipient shall safeguard all classified material and shall provide and maintain a system of security controls within its organization in accordance with the requirements of: (i) the 'Department of Defense Security Agreement' (DD Form 441), (ii) the ISM (attachment to DD Form 441), and (iii) any revisions or changes to the ISM required by the demands of national security as determined by the U.S. Government." In such situations, the official of the UA, or designee, who releases or discloses the classified information to the firm, organization, or individual shall fulfill the responsibilities which this regulation and the ISM assign to the contracting officer (such as, furnishing necessary classification guidance, authorizing retention of classified material, and certifying contractors' need to attend classified meetings).

(2) When foreign classified information is made available to a contractor by a UA in connection with a U.S. classified contract, procedures applicable to U.S. classified information shall be used. However, when foreign classified information is made available to U.S. contractors in connection with a foreign classified contract, the responsibility for the actions which this regulation and the ISM charge to the contracting officer and the contracting UA shall be as prescribed in paragraph 8-103e. Responsibilities not specifically

assigned in paragraph 8-103e are reserved to the foreign government agency or foreign contracting activity concerned.

(3) When a report is submitted in accordance with paragraph 6a (18), ISM, the CSO shall contact the originator, or, where appropriate, the authority releasing the classified material to the contractor to: (i) identify the source and contact for obtaining classification guidance relating to the material, (ii) establish the contractor's need for the material, (iii) determine the safeguards that are prescribed for the protection of the material, and (iv) determine the disposition instructions which are applicable to the material. Upon receipt of the classification guidance and disposition instructions from the releasing authority, the CSO shall provide such information to the contractor. UA's originating such material, or releasing or authorizing the release of such material to contractors, shall assist CSO's in establishing appropriate guidance and instruction for contractors who receive classified material without proper guidance for its protection and disposition.

e. Any situation or emergency which indicates a need for clarification, modification, addition, or deletion to this regulation shall be reported promptly, together with recommendations, through channels to the DIS, ATTN: Deputy Director (Industrial Security). Temporary action is authorized to be taken by a UA to safeguard its classified information in an emergency situation.

f. This regulation shall not be construed to limit in any manner the authority of the Secretary of Defense, the Secretaries of the Army, Navy, and Air Force, or the Heads of UA's individually, to grant access to classified information under the cognizance of their department or agency, to any individual designated by them. The granting of such access is beyond the scope of the DoD Industrial Security Program.

g. The Deputy Director (Industrial Security), HQ DIS is responsible for the implementation and administration of security procedures applicable to the transmission of SECRET material by commercial carriers.

h. The Commander, Military Traffic Management Command (MTMC) is responsible for the implementation and administration of security procedures applicable to the transmission of CONFIDENTIAL material by commercial carriers within the continental U.S. (CONUS). Designated Commanders will provide this service in prescribed areas outside the CONUS (also see appendix F).

i. All U.S. Arms Control Disarmament Agency (ACDA) contracts involving contractor access to RESTRICTED DATA are, by separate agreement between ACDA and the Department of Energy (DOE), the responsibility of the DOE.

1-102 Superseded Regulation. This regulation supersedes the ISR dated February 1984 and Changes thereto. *

1-103 Responsibilities. Security responsibility for contracts awarded to industry is set forth below (see section VIII for contracts awarded to foreign industry).

a. The contractor is required to comply with the security provisions of the ISM and with any additional security requirements established by the contract, regardless of the geographical location of the classified material.

b. Within the U.S., Puerto Rico, or a U.S. possession or trust territory, the Deputy Director (Industrial Security) shall assume security cognizance for all contractor facilities within the region, and shall perform CSO functions prescribed in this regulation on behalf of all UA's with respect to all contractor facilities within the region. However, in the case of contractor facilities located on a UA installation, certain security actions may be performed by the Commander or Head of the installation concerned (see paragraph 1-108). The Director of Industrial Security, Pacific Region, is assigned security cognizance for contractor facilities performing in U.S. trust territories or possessions in the Pacific area, and the Director of Industrial Security, Southeastern Region, is assigned security cognizance for contractor facilities performing in Puerto Rico, and U.S. possessions in the Atlantic and Caribbean areas. The appropriate CSO may make the necessary arrangements with the Commander or Head of the UA installation located closest to the contractor's operations to perform industrial security supervision and inspections of such operations on his or her behalf. Upon completion of the arrangement, the CSO will notify the HQ activity of the UA installation involved and the Deputy Director (Industrial Security,) HQ DIS as to the identity and the location of the Commander or activity performing the required industrial security supervision. If the above arrangements are not feasible, a security representative from the appropriate CSO shall make the required security inspections. The frequency of such inspections may be modified with the approval of the Deputy Director (Industrial Security), HQ DIS.

c. Outside the areas enumerated in paragraph b above, the UA awarding the classified contract shall assume responsibility for all security aspects of contract supervision (see paragraph 1-115) unless the UA requests this responsibility be undertaken by DIS.

d. The Director, DISCO shall assume responsibility for all industrial PCL functions prescribed by this regulation. Except in cases pertaining to owners, officers, directors, partners, regents, trustees, or executive personnel (OODEPs) which are transmitted through the CSO, contractors deal directly with DISCO on all PCL's, transfers of PCL's, and issuances of security assurances. The DISCO shall:

- (1) process and issue PCL's for contractor personnel, including those employees located on UA installations;
- (2) maintain the PSCF of contractor FCL's and PCL's;
- (3) on request, furnish PCL information on contractor employees, including those on UA installations;
- (4) on application by a U.S. contractor, make a security assurance determination predicated upon a LOC; and
- (5) advise the Commander or Head of a User Agency installation whenever the security clearance for a contractor employee, who is duty stationed with a contractor activity on his/her installation, has been suspended, denied or revoked. *

e. When shipping SECRET material by commercial carrier, UA's are responsible for obtaining the necessary routing instructions from MTMC, and for utilizing a carrier which has been qualified by MTMC and has been granted an appropriate FCL by the CSO. The MTMC, in turn, shall be responsible for assuring that a qualified carrier which has been granted an appropriate FCL by the CSO is used 1/, except where use of prepaid commercial bill of lading (CBL) has been authorized in the appropriate contract or approved by the contracting officer concerned 2/. SECRET material shall be shipped by government bill of lading (GBL) or CBL annotated thereon: "To be converted to a Government Bill of Lading." In addition, the notation, "Protective Security Service Required," shall be reflected on all copies of the bill of lading (BL). An annotated CBL must be converted to a GBL before payment is made. The BL's will be maintained in a suspense file to follow up on overdue or delayed shipments.

1-104 Arrangement of Regulation. This regulation covers the essential policies and procedures with respect to safeguarding classified information. It is divided into sections, parts, and paragraphs. Each section is designated by subject and Roman numerals (for example, I, II, and III), and covers a separate aspects of industrial security. The parts are designated by title and Arabic numerals (for example, 1, 2, 3), and contain a breakdown of the subject covered by the section into related divisions. The paragraphs are a further division of the parts. They are so numbered that the first digit indicates the section; the second digit, the part; and the last two digits, the paragraph (for example, 2-103, designates section II, part 1, paragraph 3; 3-314 designates section III, part 3, paragraph 14). The regulation is designed to permit subsequent insertions of additional parts and paragraphs within the appropriate section.

1-105 Amendment of Regulation. This regulation will be amended from time to time. Unless otherwise specified in any amendment, compliance with an amendment shall not be mandatory until 30 days after date of publication, although compliance shall be authorized from the date of its publication.

1-106 Distribution and Use of Regulation. This regulation is intended for the use and guidance of industrial security and procurement activities of the UA's. It shall be distributed through normal channels to staff and operating activities concerned with industrial security and procurement matters. This regulation is not applicable to industrial management, and is not intended for distribution to industry. Parts or all of this regulation may be made available to industrial management, when judged to be in the interest of a UA.

1/ Non-DoD UA's may issue their own routing instructions; however, when doing so they will ensure that only commercial carriers which have been qualified by MTMC and granted an appropriate FCL by the CSO are utilized.

2/ In such cases, the SECRET shipment shall be routed via a cleared commercial carrier under a tariff, tender, or contract that provides PSS in accordance with DoD 5220.22-C (reference (b)).

1-107 User Agency Procedures Under This Regulation. UA's may augment this regulation by prescribing more detailed regulations and operating instructions as may be required and which are not inconsistent with this regulation. The application of these procedures shall be guided by the twofold objective of establishing uniformity and maintaining maximum security, consistent with the accomplishment by each UA of its assigned mission. Two copies of each implementing regulation or instruction issued by a UA shall be furnished to Director, DIS, ATTN: Deputy Director (Industrial Security) for information.

1-108 Contractor Activities on a User Agency Installation.

a. The Commander or Head of a UA installation shall provide security supervision of contractors and their employees located on the installation as follows.

(1) For installations located outside of the U.S., Puerto Rico, or a U.S. possession or trust territory, the contractor and his or her employees shall be considered to be visitors. In such cases the procedures set forth in paragraph e below shall apply.

(2) For installations located within the U.S., Puerto Rico, or a U.S. possession or trust territory, the contractor and his or her employees shall be considered to be visitors, or the Commander or Head of the installation may elect to declare the contractor activity a facility under one of the following criteria if:

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

(b) the contractor's operation is to be of a quasi-permanent nature;

(c) the contractor maintains management control over his or her operations; or

(d) the contractor is in a position to maintain separate security procedures.

FCL's shall not be established on the installation solely for the purpose of permitting a contractor entry authorization into a controlled area unless access to classified information is required in the performance of the contract.

b. If, in light of the foregoing, the Commander or Head of the UA installation decides that the contractor's on-installation activity requires a FCL, he or she shall request the CSO in whose geographical area the installation is located (see appendix B for listing of CSO's and boundaries) to assume security cognizance of the facility. The Commander or Head of the installation shall request the CSO to perform all cognizant security functions provided for in this regulation, or he or she shall notify the CSO in writing that he or she has elected to perform the following security actions.

(1) Accomplish the FCL survey and furnish the CSO a copy of the "Facility Security Clearance Survey" (DD Form 374), the DD Form 441 or the "Appendage to Department of Defense Security Agreement" (DD Form 441-1), the "Certificate Pertaining to Foreign Interests" (DD Form 441s), and exclusion certificates, as required.

(2) Assure that the contractor has prepared a standard practice procedure (SPP), covering the contractor's operations on the UA installation.

(3) Assure that the contractor observes required security controls through periodic inspections in accordance with the schedule prescribed by paragraph 4-103, and furnish to contractors letters of requirements resulting from such inspections, if appropriate.

(4) Assure that the contractor maintains management control over his or her operations.

(5) Assure that prompt remedial action is taken where security conditions are deficient in the contractor's operations.

(6) Review, when appropriate, contractor control of incoming visitors to contractor facilities on the installation.

(7) Ensure that the DoD security education program is implemented by the contractor and, as required, conduct defensive security briefings required by paragraph 5u, ISM.

(8) Conduct investigation of contractor security violations, including loss, compromise, or suspected compromise of classified information in accordance with section V. If the services of a governmental investigative agency are required, request services from the appropriate military investigative agency.

(9) Furnish to the facility, guidance on the application of security requirements including establishment or disestablishment of closed or restricted areas. Requests from the contractor for interpretations of the requirements of the ISM shall be forwarded to the CSO.

(10) Request from DISCO interim PCL's for contractor personnel when required to prevent crucial delay in the negotiations or performance of the contract.

(11) Assure that the contractor reports promptly to the CSO and the Commander or Head of the UA installation any incidents which involve espionage, sabotage, subversive activity, or the loss, compromise, or suspected compromise of classified information.

(12) Recommend to the CSO the termination, revocation, or suspension of the FCL, as appropriate.

(13) Conduct the briefing and debriefing of the facility security supervisor (FSO), the COMSEC custodian, and alternate COMSEC cus- *

todian when there is a COMSEC account or there is a requirement to establish a COMSEC account (see paragraph 2-313). Brief and debrief only the FSO if no COMSEC account is required. *

c. When the security actions outlined in paragraph b above are performed by the Commander or Head of the installation, the following actions shall be accomplished by the CSO.

(1) Grant the FCL to the contractor provided the preclearance survey has been completed and the required forms are in order.

(2) Assign an industrial security specialist to accompany the installation security inspector during special or scheduled inspections upon request or as otherwise appropriate after coordination with the Commander or Head of the UA installation.

(3) Verify FCL and safeguarding ability, when requested (see paragraph 1-110b). *

(4) Terminate, revoke, or suspend FCL's, as appropriate.

d. Reports of initial "Facility Security Clearance Survey," recurring inspections reported on "Industrial Security Inspection Report" (DD Form 696), letters of requirements to the contractor, and reports resulting from investigations conducted in accordance with section V shall be exchanged between the Commander or Head of the UA installation and the CSO.

e. If the Commander or Head of the UA installation does not elect to clear contractors on his or her installation as facilities, he or she shall provide appropriate security supervision and shall be responsible for the following:

(1) Provide written instructions specifying: (i) those security actions which will be performed for the contractor by the installation such as providing storage facilities, guard service, mail and freight services, and visit control, and (ii) those security actions for which joint action may be required such as the packaging and addressing of classified transmittals, and control of visitors.

(2) Ensure that the contractor has prepared a SPP covering the contractor's activities on the UA installation, if appropriate.

(3) Ensure that the contractor observes required security controls through periodic inspections in accordance with the schedule prescribed by paragraph 4-103, and furnish to contractors letters of requirements resulting from such inspections, if appropriate.

(4) Ensure that prompt remedial action is taken when security conditions are deficient in the contractor's operation.

(5) Ensure that the DoD security education program is implemented by contractors and, as required, conduct defensive security briefings required by paragraph 5u, ISM.

(6) Conduct investigation of contractor security violations, including loss, compromise, or suspected compromise of classified information.

(7) Conduct the briefing and debriefing of the FSO, the COMSEC custodian, and alternate COMSEC custodian when there is a COMSEC account or there is a requirement to establish a COMSEC account (see paragraph 2-313). Brief and debrief only the FSO if no COMSEC account is required. *

(8) Furnish to the contractor guidance on the application of security requirements to the contractor's operations.

(9) Forward requests from the contractor for interpretations of the ISM to the CSO.

(10) Request from DISCO interim PCL's for contractor personnel, when required, to prevent crucial delay in the performance of the contract.

(11) Ensure that the contractor reports promptly any incidents which involve espionage, sabotage, subversive activity, or the loss, compromise, or suspected compromise of classified information. In addition, the CSO of the visiting contractor's facility shall be advised concerning the incident.

f. For those installations located outside of the U.S., Puerto Rico, or a U.S. possession or trust territory, where the Commander or Head of the UA installation has relinquished security responsibilities to DIS, the Office of Industrial Security International (OISI) and/or the appropriate CSO will be responsible for assuring that the security actions outlined in paragraph 1-108e above are accomplished.

1-109 Expenditure of Funds for Security. The CSO shall not commit the government to reimburse the management of a facility for funds expended in connection with the facility's security program. In the case of a cost-reimbursement-type contract, the allowability of security costs is determined by the contracting officer in accordance with the terms of the contract and with the cost principles of the Federal Acquisition Regulation (FAR) (reference (gg)). Under a fixed price contract, the initial contract price includes all applicable security costs. An equitable adjustment may be made in the initial contract price when, as indicated in the contract security clause, the security classification or security requirements under the contract are changed by the government and the change results in an increase or decrease in the contract price.

1-110 Disclosure of Classified Information to a Contractor by User Agency Contracting Activities.

a. Prior to the disclosure of any classified information to a facility, the contracting activity of the UA shall determine that the contractor's facility has a valid FCL equal to, or higher than, the category of classified information to be disclosed. If the facility will be required to have physical possession of classified material, the contracting activity shall also determine that the facility has the ability to properly safeguard the classified information to be disclosed to, or developed by, the facility.

(This determination may be made at the same time as the FCL verification.)
Such determinations shall be based on:

(1) the contracting activity's knowledge of the ability of the facility to adequately safeguard the material to be developed or released, based upon a current contractual relationship involving classified material of the same or higher category as that to be released or developed under the new contract or program; or

(2) the written verification by the Personnel Investigations Center (PIC) - Central Verifications Activity (CVA), 3/ mailing address: *

Defense Investigative Service *
PIC-CVA *
P.O. Box 1211 *
Baltimore, MD 21203-1211 *
Telephone Number: (301) 633-4820 *

or the CSO if appropriate, of the safeguarding ability of the facility in the event that the procuring contracting activity does not have the knowledge required in paragraph (1) above. In this connection, the contracting activity shall furnish to the PIC-CVA or CSO of the facility information available (description, quantity, end item, and classification of the information related to the proposed contract or program, and any other facts) to assist the PIC-CVA or CSO in making such a determination. *

b. The PIC-CVA, or the CSO if appropriate, shall furnish written verification to the contracting activity as to whether a facility has an appropriate FCL and has the appropriate safeguarding capability for the classified material involved. Unless otherwise notified (superseded) in writing by the PIC-CVA or CSO, each verification furnished in accordance with this paragraph shall remain valid for a period of 1 calendar year from the date of issuance. In the event a FCL has not been issued, the requester shall be so advised. Further action shall not be taken unless a formal request to clear the facility is received by the CSO. *

c. The verification of safeguarding ability furnished by the PIC-CVA or CSO shall be based upon inspections conducted in accordance with this regulation, or in the event the facility is not on the current inspection schedule, upon a visit which has been made to the facility to obtain the required data. Written verification shall be dispatched within 5 working days from receipt of inquiry. *

3/ Under the following circumstances, the PIC-CVA will not be able to respond and requesters shall make inquiries to the appropriate CSO: *

(i) requests involving the transfer of material that would require more than two cubic feet of storage, (ii) requests involving commercial carriers under the provision of paragraph 17c(5)(c), Industrial Security Manual, and (iii) requests for certification of security clearance and safeguarding ability to the Defense Technical Information Center. *

d. In the event the FCL must be revalidated or raised to an appropriate level, or the facility must provide adequate safeguards in order to comply with the requirements of the ISM, the requester shall contact the CSO which will advise them of the nature of such actions, and of the estimated time required to complete such actions. Moreover, the requester shall be asked to advise as to whether the CSO should initiate action to have the FCL revalidated or raised to an appropriate level. Additional action shall not be taken by the CSO unless the requester advises that it is necessary to bring the FCL to a valid status. In such cases, appropriate action shall be initiated promptly by the CSO and the requester shall be informed when action is completed. *

e. When noncontract-related classified material is released under a Scientific and Technical Information Release Program, or a classified contract is awarded which requires classified reports to be disseminated to other individuals or firms in accordance with a standard mailing or distribution list, the sponsoring, releasing, or contracting activity, as appropriate, has the following responsibilities in order to make certain the intended recipients are eligible to receive the classified information.

(1) Verify initially the need-to-know, FCL, and safeguarding capability of the recipients of the reports, unless this requirement is levied on the prime contractor.

(2) Ensure that the recipients of classified material are provided appropriate classification guidance and instructions, to assure proper identification, control, accountability, handling, protection, and ultimate disposition of classified information, to include specific retention authority, which the individual or company may be required to use in its operations and for discussions involving classified information.

(3) Notify appropriate PIC-CVA, or appropriate CSO(s), if applicable, and the prime contractor of any change in the mailing list. *

(4) Require in the contract or other appropriate written notification that the releasing activity or the prime contractor making the distribution of the reports determines the storage and safeguarding capability of the recipient from the PIC-CVA, or appropriate CSO, if applicable, prior to making the first release of any reports. Subsequent releases of material may be made without reverification of storage and safeguarding ability until such time as the distribution list is revised to delete the recipient. *

f. The FCL verification notification shall be retained for one year, after which it shall be destroyed. The recipient of the verification notification shall be immediately notified should a change occur adversely affecting the level of the FCL or the safeguarding ability of the facility. *

g. The DISCO shall not verify FCL's or safeguarding ability. This information shall be obtained from the PIC-CVA or the CSO of the facility, if applicable. *

1-111 Disclosure of Classified Information to a Subcontractor by a Prime Contractor.

a. Prior to the disclosure of any classified information to a subcontractor, the prime contractor shall determine that the subcontractor has a valid FCL equal to or higher than the category of classified information to be disclosed, unless there is an existing contractual relationship between the parties involving classified information of the same or higher category as that to be released or developed under the new subcontract. A prime contractor, having verified a prospective subcontractor's FCL, shall obtain the written approval of the contracting office of the prime contract concerned, prior to disclosure of TOP SECRET information 4/ to the prospective subcontractor. *

b. If the prospective subcontractor will be required to have physical possession of TOP SECRET, SECRET, or CONFIDENTIAL material during the precontract or performance stages of the classified subcontract, the prime contractor shall, in addition to verifying the subcontractor's FCL, also determine that the subcontractor has the ability to safeguard properly the classified information to be released or developed under the subcontract. Such determination shall be based on:

(1) the prime contractor's knowledge of the ability of the prospective subcontractor to safeguard adequately the material to be released and produced, based upon a current contractual relationship involving classified material of the same or higher category as that to be released or developed under the new subcontract, or

(2) the written verification from the PIC-CVA, or the CSO * if appropriate of the safeguarding ability of the prospective subcontractor, in the event the prime contractor does not have the knowledge required in paragraph (1) above. In this connection, the prime contractor shall furnish the PIC-CVA or if appropriate, the CSO of the prospective subcontractor * information available to him or her (such as description, quantity, end item, and classification of the information related to the proposed subcontract, and any other facts) in order to assist the PIC-CVA or CSO in making such a * determination.

4/ A contractor is not authorized to release classified intelligence information * to a subcontractor, vendor, or supplier without proper written authorization of the contracting UA. All classified intelligence information, whether obtained during a visit or through other sources, shall be safeguarded and controlled in accordance with the provisions of the ISM, with any additional instructions which may be received from the releasing UA activity and any specific restrictive markings or limitations appearing on documents. All inquiries concerning source, acquisition, use, control, or restrictions pertaining to intelligence information shall be directed to the contracting UA activity concerned. This activity shall either handle the inquiry or arrange with other authorized releasing activities within the UA to handle the inquiry and provide guidance as requested.

(3) The PIC-CVA, or the CSO if appropriate, shall advise *
the requesting prime contractor of the current FCL status and safeguarding
ability of the prospective subcontractor as prescribed in paragraphs 1-110c,
d, e, and f.

1-111.1 Disclosure of Critical Nuclear Weapon Design Information (CNWDI).

a. Prime Contractors. When a contracting officer has a requirement to release CNWDI information to a contractor, the CSO will be so advised and requested to brief the FSO and his or her alternate. In addition to the other requirements established for the release of classified information to contractors, CNWDI shall not be released unless the FSO and his or her alternate have been briefed by the CSO. The briefing shall include the definition of CNWDI, a reminder as to the extreme sensitivity of the information, and an explanation of the individual's continuing responsibility for properly safeguarding CNWDI and for ensuring that dissemination is strictly limited to other personnel who have been authorized for access and have a specific need-to-know for the particular information. The CSO shall maintain a record stating that the FSO and his or her alternate have been briefed and that the facility is authorized for access to CNWDI. Verification of the facility's eligibility for access to CNWDI may be obtained from the PIC-CVA, or the CSO if appropriate, or the *
determination of the facility's eligibility may be based on the contracting activity's knowledge based upon a current classified contract with the contractor involving access to CNWDI.

b. Subcontractors. Contracting officers shall authorize prime contractors to release CNWDI to subcontractors, only after it has been determined that the subcontractor FSO and his or her alternate have been briefed as required in paragraph a above. The CSO shall also maintain a record that the facility is authorized access to CNWDI in the same manner as provided in paragraph a above. Similarly, verification of the facility's eligibility for access to CNWDI may be verified through the PIC-CVA, or the CSO if appropriate, or *
based upon a current classified contract with the subcontractor involving access to CNWDI.

c. Consultants. Type A Consultants may be briefed and afforded access to CNWDI, but such access may be permitted only at the facility of the contractor who engaged the Type A Consultant or at the government contracting activity. Type B and C Consultants shall not be briefed or afforded access to CNWDI without the prior approval of the contracting officer.

1-112 Applicability to Subcontractors and Their Employees. The procedures established in this regulation pertaining to contractors and their employees are equally applicable to subcontractors, vendors, or suppliers and their employees and, in turn, to each succeeding tier of subcontractors. Each subcontractor will be regarded by the DoD to be in the same category as a prime contractor with respect to his or her individual subcontractors.

1-113 Public Disclosure. In accordance with paragraph 5o, ISM, *
contractors are precluded from releasing, for public dissemination, *
information pertaining to classified contracts or programs, except after *
approval by the Directorate for Security Review, Office of the Assistant *

Secretary of Defense (Public Affairs) (OASD(PA)).5/ In the review for approval for public release, a determination must be made to ensure: (i) that classified information is not contained in the proposed release, (ii) that unclassified information which might not be in the national interest, such as militarily critical technology, is not revealed in the proposed release, and (iii) that the limitations and policies governing unclassified technical data under the International Traffic in Arms Regulation (ITAR) or the Export Administration Regulations (EAR) 6/ are adhered to.7/ DoD Directive 5230.9 (reference (d)), establishes policies and procedures, and assigns responsibilities governing the review and clearance of information proposed for public release by DoD.

a. DoD 5230.9 directs, inter alia, that information for public release shall be submitted to OASD(PA) for review and clearance prior to disclosure if the information:

(1) originates or is proposed for publication or release at the Seat of Government; or

(2) meets any of the following criteria:

(a) is or has the potential to become an item of national or international interest or has foreign policy or foreign relations implications;

(b) concerns high level military or DoD policy or U.S. Government policy;

(c) concerns subjects of potential controversy among DoD Components or with other federal agencies;

(d) concerns the following subject areas:

5/ If the information pertains to a classified contract or program awarded by a non-DoD agency, requests for approval for release shall be submitted to that non-DoD agency.

6/ Part 379 of the Export Administration Regulations and Section 125 of the International Traffic in Arms Regulation, are applicable.

7/ Release of unclassified technical data is governed by the Export Administration Act of 1979, administered by the Department of Commerce, and the Arms Export Control Act of 1976, administered by the Department of State through the International Traffic in Arms Regulation. After information is reviewed for security and determined to be unclassified, a further determination must be made for compliance with the export laws and regulations before it is finally approved for public release. This review is necessary because approval for public release may negate the requirement to obtain an export license for that information.

1. new weapons or weapons systems of significant modifications or improvements to existing weapons or systems, equipment, or techniques; *

2. military operations, operations security, potential operations, and significant exercises; *

3. national command authorities and command posts; *

4. military applications in space, nuclear weapons, including nuclear weapons effects research, chemical warfare, defensive biological and toxin research, and high energy lasers and particle beam technology; *

5. material involving critical military technology (see paragraph 1.221.2); *

6. communications security, signals intelligence, and computer security; and *

7. others as the OASD(PA) may designate. *

b. Heads of DoD Components have clearance authority for information not specified in paragraph a above, and may delegate this authority to the lowest echelon competent to evaluate the content and implications of the information. Reviewing officials in the User Agencies must understand their responsibility for identifying the information specified in paragraph a above, which must be reviewed by higher authority to determine its releasability. User Agencies should refer all doubtful cases to higher authority or to OASD(PA) for resolution. *

c. It is the policy of the DoD that the university community, engaged in classified research work, be permitted to publish with minimum delay, the unclassified results of such research. To ensure the expeditious processing of such information, no delay of more than 30 days shall elapse from date of receipt without dispatch of an explanatory communication to the submitting college or university by the reviewing command or other authority. Denial of clearance of an entire paper or other material should be avoided when it is possible to approve clearance, with amendments, to eliminate identified security information. *

1-114 Waivers, Special Access Programs, and Carve-Outs. *

a. The DUSD(P), his or her designee, or higher authority, shall provide overall policy guidance to this program and shall approve waivers to, or deviations from, the DoD security policy promulgated in this regulation and in the ISM. The Director, DIS (or when absent, the Acting Director) may approve waivers to, or deviations from, the provisions of this regulation or the ISM which do not require action by the DUSD or designee. All requests for waivers or deviations, including supporting justification, shall be submitted to the Director, DIS, ATTN: Deputy Director (Industrial Security) through the appropriate CSO.

b. Executive branch agency heads who are designated by the President of the U.S. as original TOP SECRET classification authorities pursuant to E.O. 12356 (reference (w)) may establish special access programs with special access, distribution, or protection requirements beyond those normally provided for access to TOP SECRET, SECRET, or CONFIDENTIAL information. Such officials or their designees shall make these programs applicable by incorporation in the contract or other appropriate notification and by providing copies of these to the CSO.

c. The Secretaries of the Military Departments and the Heads of DoD Agencies shall make the approved special access program requirements applicable by incorporating them in the contract and furnishing a copy of the requirements to the CSO.

d. To the extent required by the Director, DIS to execute his or her security responsibilities with respect to contracts, the UA shall provide for the granting of authorization for access to special access programs by DIS industrial security personnel.

e. Additional investigative requirements shall not be required by UA's for any project or program, other than those established herein, without the prior approval of the DUSD(P), his or her designee, or higher authority.

f. The use of "carve-out" contracts, which relieve the DIS from inspection responsibility under the Defense Industrial Security Program, is prohibited unless such contracts are in support of approved Special Access Programs.^{8/} In these instances, the User Agency shall provide a copy of DD Form 254, "Contract Security Classification Specification," to the appropriate cognizant security office and indicate in Item 15, what agency will have the inspection responsibility for the carve-out contract. Specific elements and areas which are "carved-out" shall also be specified. *

1-115 Security Administration of U.S. Classified Contracts Awarded to U.S. Contractors for Performance Abroad. The security administration of a U.S. classified contract awarded to a U.S. contractor which will require performance outside of the U.S., Puerto Rico, or a U.S. possession, territory, or trust territory will be accomplished as follows.

a. The Director of Industrial Security for the DIS Region in which the HOF or principal U.S. based office of the contractor is located shall assume security cognizance of the contractor. The functions to be performed by the CSO will encompass all the usual aspects of security cognizance established by this regulation as they pertain to the contractor's U.S. based facility. This will include the processing of the contractor for a FCL; that is, the execution of the DD Form 441; the DD Form 441s; the resolution of all questions involving foreign ownership, control, or influence (FOCI), in accordance with this regulation; and the processing of all OODEPs *

^{8/} DoD Components must comply with Chapter XII, "Special Access Programs" of DoD 5200.1-R, "Information Security Regulation." Non-DoD User Agencies must comply with their Agency procedures and regulations. *

for PCL's pursuant to this regulation. In this connection, the contractor's SPP which relates to the contractor's overseas operation will be routed through the UA to the CSO for review. (All aspects of security administration which must be performed outside of the U.S., Puerto Rico, or a U.S. possession, territory, or trust territory, most notably the inspection function, will be the responsibility of the UA as discussed in paragraph c below, unless the UA requests this responsibility be assumed by DIS. The DIS will assume this responsibility upon receipt of such a request identifying specific U.S. installations. Requests for such support should be submitted to the Director, DIS, ATTN: Deputy Director (Industrial Security)).

b. The Director, DISCO shall be responsible for the industrial PCL function prescribed by this regulation regardless of where the contractor's employees are physically located. In this regard, all LOC's will be issued to the contractor's U.S. based cleared facility.

c. The UA awarding the contract shall be responsible for adapting, as may be necessary, the provisions of this regulation and the ISM to its classified contracts performed by the contractor on a UA installation outside the U.S., Puerto Rico, or a U.S. possession, territory, or trust territory. In the event a contractor is working on classified contracts of two or more UA's at one location, or is performing on a classified contract awarded by one UA for performance on another UA installation, the UA's concerned and, if appropriate, DIS shall develop mutually acceptable arrangements for the fulfillment of the responsibilities set forth in this paragraph. These responsibilities include all inspections of overseas sites where the contract is being performed. The basic security requirements imposed on the contractor are set forth in the ISM. In this connection, however, the UA is responsible for including in the contract, or other appropriate notification, any physical security requirements which are in addition to the ISM and which are necessary by virtue of the foreign location at which the classified contract is being performed. This would include specific requirements regarding the storage of classified information on government installations and the transmission of classified information through U.S. Government controlled channels. In such cases, the contracting UA shall furnish the additional security requirements to the CSO of the contractor's U.S. based facility, and the DIS activity responsible for inspections. In addition, the contracting UA shall include in the contract, or other appropriate notification, any special access program requirements established by the Secretary or Head of such UA (see paragraph 1-114), and furnish notice of the additional access requirements to the CSO of the contractor's U.S. based facility and the DIS activity having inspection responsibility.

d. A contractor activity located outside of the U.S., Puerto Rico, or a U.S. possession, territory, or trust territory shall not be granted a FCL in accordance with this regulation.

1-116 Privileged Information.

a. Reports submitted or information provided pursuant to the requirements of subparagraphs 5aa; 6a(1), (2), and (3); and 6b(1), of the ISM either classified if they so qualify, or offered in confidence and so

marked by the contractor, will be treated as privileged. When such reports are submitted in confidence, applicable exemptions of DoD 5400.7-R (reference (1)) will be invoked as a matter of policy to withhold them from public disclosure. Such reports, other than those already classified, will be marked "FOR OFFICIAL USE ONLY," following their receipt and determination that they fall within one of the exemptions.

b. When reports submitted pursuant to the requirements of the ISM cited in paragraph a above contain unclassified information pertaining to an individual, it may not be withheld from that individual under the provisions of DoD 5400.11-R (reference (m)), except that the identity of a source who furnished information to the government under an express promise of confidentiality may be protected by necessary deletions from that information. An implied promise of confidentiality given prior to September 27, 1975 is an adequate basis for deleting that information which identified its confidential source.

c. Should action for defamation of character be brought against a contractor or its employees for reporting information concerning an individual in accordance with the requirements of the ISM cited in paragraph a above, and the defendants in the suit seek the assistance of DoD in defending against the suits, their request should be referred to the Office of the Deputy Assistant Secretary of Defense (Security Policy) (ODASD(SP)), Office of the Assistance Secretary of Defense (Comptroller) (OASD(C)), for appropriate action.

Part 2. DEFINITION OF TERMS

1-200 Definitions. The definitions set forth below are established for the purpose of this regulation.

1-201 Access, Accessibility. This refers to the ability and opportunity to obtain knowledge of classified information. An individual, in fact, may have access to classified information by being in a place where such information is kept, if the security measures which are in force do not prevent him or her from gaining knowledge of the classified information 9/. *

1-202 Accountable COMSEC Material. COMSEC material received, sent, and controlled under the COMSEC Material Control System is considered accountable COMSEC material. Such material is normally identified by a short title assigned under the Telecommunication Security (TSEC) nomenclature system.

9/ The entry into a controlled area, per se, will not constitute access to classified information if the security measures which are in force prevent the gaining of knowledge of the classified information. Therefore, the entry into a controlled area under conditions that prevent the gaining of knowledge of classified information will not necessitate a PCL. *

1-203 Alien. Any person not a citizen or national of the U.S. (see "Immigrant Alien," paragraph 1-237) is considered an alien.

1-204 Authorized Persons. Those persons who have a need-to-know for the classified information involved, and have been cleared for the receipt of such information (see paragraph 1-239) are authorized persons. Responsibility for determining whether a person's duties require that he or she possess, or have access to, any classified information, and whether he or she is authorized to receive it, rests on the individual who has possession, knowledge, or control of the information involved, and not on the prospective recipient.

1-205 Candidate Material. That material which is referred to collectively as special nuclear materials and nuclear weapons is candidate material.

1-205.1 Carve-Out. A classified contract issued in connection with an approved Special Access Program in which the DIS has been relieved of inspection responsibility in whole or in part. *

1-206 Central Office of Record (COR). The activity within a department or agency charged with the responsibility for maintaining records of accountability of all accountable COMSEC material received by or generated within the department or agency is the COR.

1-207 Channels for the Dissemination of COMSEC Material.

a. COMSEC Distribution and Accounting Channels. This refers to the distribution channels or shipping routes through which the COMSEC material is handled and shipped so that from the time of origin to eventual disposition the material is moved under a continuous receipt system from COMSEC custodian to COMSEC custodian. These channels are referred to as the COMSEC material control system.

b. Classified Information Channels. This refers to normal classified information channels through which classified COMSEC correspondence and matter other than accountable COMSEC material is transmitted.

1-208 Classified Contract. Any contract that requires or will require access to classified information by the contractor or his or her employees in the performance of the contract is a classified contract. (A contract may be a classified contract even though the contract document is not classified.)

1-208.1 Classification Guide. A document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specified information to be classified derivatively is a classification guide.

1-209 Classified Information. This refers to information or material that is: (i) owned by, produced by or for, or under the control of the U.S. Government; (ii) determined under E.O. 12356 or prior orders to require protection against unauthorized disclosure; and (iii) so designated.

1-209.1 Classifier. An individual who makes a classification determination and applies a security classification to information or material is a classifier. A classifier may be a classification authority or may derivatively assign a security classification based on a properly classified source or a classification guide. Within this context, contractors may apply security classification markings based on classified source material or a DD Form 254, as required by this regulation.

1-210 Closed Area. A closed area is a controlled area established to safeguard classified material which, because of its size or nature, cannot be adequately protected by the safeguards prescribed in paragraph 16, ISM, or be stored during nonworking hours in accordance with paragraph 14, ISM, (see section IV, ISM).

1-211 Cognizant Security Office (CSO). This refers to the office of the DIS Director of Industrial Security that has industrial security jurisdiction over the geographic area in which a facility is located.

1-212 Colleges and Universities. This refers to all educational institutions which award academic degrees, as well as related research activities directly associated with a college or university through organization or by articles of incorporation.

1-213 Reserved.

1-214 Communications Intelligence. This is technical and intelligence information derived from foreign communications by other than the intended recipients.

1-215 Communications Security (COMSEC). COMSEC refers to protective measures taken to deny unauthorized persons information derived from telecommunications related to national security and to ensure the authenticity of such communication. Such protection results from the application of security measures to electrical systems generating, handling, processing, or using national security information and also includes the application of physical security measures to COMSEC information or materials.

1-216 Communications Security (COMSEC) Information. COMSEC information is all information concerning COMSEC and all COMSEC material. (This includes classified information pertaining to COMSEC but not sent, received, or safeguarded within the COMSEC material control system. Examples are COMSEC installation standards, material, and classified design information produced under contract which will become CRYPTOSYSTEM/COMSEC materials upon acceptance by the U.S. Government.)

1-217 Compromise. Compromise is the disclosure of classified information to persons not authorized access thereto.

1-217.1 Compromising Emanations. This refers to unintentional or intelligence-bearing signals which, if intercepted or analyzed, disclose national security information transmitted, received, handled, or otherwise processed by any information processing system.

1-218 CONFIDENTIAL. "CONFIDENTIAL" is the designation that shall be applied to information or material the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

1-219 Continental Limits of the United States. This refers to U.S. territory, including the adjacent territorial waters located within the North American continent between Canada and Mexico.

1-220 Contracting Officer. A contracting officer is any person who, in accordance with departmental 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 thereto, or any part of such authority. The term also includes the authorized representative of the contracting officer acting within the limits of his or her authority. For purposes of this regulation and the ISM, the term contracting officer refers to the contracting officer at the purchasing office who is identified as the PCO and the contracting officer at a contract administration office who is identified as the ACO. Normally, the responsibilities which the regulation assigns to the contracting officer during the precontract, contract award, and postcontract stages of a classified procurement will be performed by the PCO, with the ACO performing those responsibilities which arise during the performance stages of a classified contract. Postcontract responsibilities include those industrial security actions which the purchasing office assumes when it authorizes a contractor to retain classified material after the termination or completion of a classified contract.

1-221 Contractor. A contractor is any industrial, educational, commercial, or other entity that has executed a "Department of Defense Security Agreement" (DD Form 441) with a DoD Agency for the purpose of performing on a classified contract or other classified procurement.

1-221.1 CNWDI. CNWDI is TOP SECRET RESTRICTED DATA or SECRET RESTRICTED DATA revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munition, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and totally contained quantities of fissionable, fusionable, and high-explosive materials by type. Among these excluded items are the components which DoD personnel, including contractor personnel, set, maintain, operate, or replace.

1-221.2 Critical Technology. Militarily-significant technology that is not possessed by potential adversaries and which, if acquired by them, would permit a substantial advance in their military capabilities, much to the detriment of the U.S. National Security. Critical technology satisfies one or more of the following criteria: *

a. it contributes to the superior characteristics (performance, reliability, maintainability or cost) of current military systems; *

b. it relates to specific military deficiencies of a potential adversary and would contribute significantly to the enhancement of their military mission; *

c. It is an emerging technology with high potential for having a major impact upon advanced weapons systems. *

(The Military Critical Technologies List (MCTL) is a reference document to be used in making this judgment). *

1-222 CRYPTO. CRYPTO is a marking or designator identifying all COMSEC keying material used to protect or authenticate telecommunications carrying national security-related information. (The CRYPTO marking also identifies COMSEC equipment with installed hardwired operational keying variables.)

1-223 CRYPTOSYSTEM. This refers to the associated items of COMSEC equipment or material used as a unit to provide a single means of encryption or decryption.

1-223.1 Custodian. An individual who has possession of or is otherwise charged with the responsibility for safeguarding or accounting for classified information is the custodian.

1-224 Declassification. This is the determination that classified information no longer requires, in the interests of national security, any degree of protection against unauthorized disclosure, coupled with a removal or cancellation of the classification designation.

1-225 Department of Defense. DoD refers to the Office of the Secretary of Defense (including all boards, councils, staffs, and commands), DoD agencies, and the Departments of the Army, Navy, and Air Force (including all of their activities).

1-225.1 Derivative Classification. This is a determination that information is in substance the same as information currently classified and the application of the same classification marking.

1-226 Document. A document is any recorded information, regardless of its physical form or characteristics, exclusive of machinery, apparatus, equipment, or other items of material. The term includes, but is not limited to, the following: all written material, whether handwritten, printed, or typed; all photographs, negatives, exposed or printed films, and still or motion pictures; all data processing cards or tapes; maps; charts; paintings; drawings; engraving; sketches; working notes and papers; all reproduction of the foregoing by whatever process reproduced; and sound/voice of electronic recordings in any form.

1-227 Downgrade. To downgrade is to determine that classified information requires, in the interests of national security, a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such a lower degree of protection.

1-227.1 Essential Elements of Friendly Information (EEFI). Key questions, or critical information/secrets about United States intentions, military capabilities, plans or programs needed by an adversary to relate with other available information and intelligence in order to assist that *

adversary in reaching a logical decision. DoD military components refer to the Essential Elements of Friendly Information as EEFI. These EEFI may be disclosed through OPSEC indicators. *

1-228 Executive Personnel. This refers to those individuals in managerial positions other than owners, officers, or directors who administer the operations of the facility. (This category includes such designations as general manager, plant manager, plant superintendent, or similar designations, the FSO, and any individual who exercises control over the FSO.) *

1-229 Facility. A facility is a plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, which, when related by function and location, form an operating entity. (A business or educational organization may consist of one or more facilities as defined above). For purposes of industrial security, the term does not include UA installations. *

1-230 Facility Security Clearance (FCL). This is an administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category (and all lower categories).

1-231 Foreign Government Information. This is information that is: (i) provided to the U.S. by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or (ii) produced by the U.S. pursuant to, or as a result of, a joint arrangement with a foreign government or governments, or an international organization of governments, requiring that the information, the arrangement, or both, are to be held in confidence.

1-231.1 Foreign Interest. The term refers to any foreign government or agency of a foreign government; any form of business enterprise organized under the laws of any country other than the U.S., or its possessions; or any form of business enterprise organized or incorporated under the laws of the U.S., or a state or other jurisdiction of the U.S., which is owned or controlled by a foreign government, firm, corporation, or person. Included in this definition is any natural person who is not a citizen or national of the U.S. (An immigrant alien as defined in paragraph 1-237 is excluded from the definition of a foreign interest.)

1-232 Foreign Nationals. All persons not citizens of, not nationals of, nor immigrant aliens to the U.S. are foreign nationals.

1-233 FORMERLY RESTRICTED DATA. This is information removed from the RESTRICTED DATA category upon joint determination by DOE (or antecedent agencies) and DoD that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information. For purposes of foreign dissemination, however, such information is treated in the same manner as RESTRICTED DATA.

1-234 Graphic Arts. This refers to facilities and individuals engaged in performing consultation, service, or the production of any component or end product which contributes or results in, the reproduction of classified information. Regardless of trade names or specialized processes, it includes writing, illustrating, advertising service, copy preparation, all methods of printing, finishing services, duplicating, photocopying, and film processing activities.

1-235 Handling. Handling refers to the preparation, processing, transmission, and custody of classified information.

1-236 Home Office (HOF). The headquarters facility of a MFO (see paragraph 1-246) is the HOF.

1-237 Immigrant Alien. Any person lawfully admitted into the U.S. under an immigration visa for permanent residence is an immigrant alien (see paragraph 2-308 for special prerequisites for clearance of immigrant aliens).

1-238 Industrial Security. That portion of internal security which is concerned with the protection of classified information in the hands of U.S. industry is industrial security.

1-239 Information Security. This refers to the result of any system of administrative policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information the protection of which is authorized by executive order or statute.

1-240 Intelligence. Intelligence is the product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of foreign operations and which is immediately or potentially significant to military planning and operations.

1-241 Interim Security Clearance. This is a security clearance based on lesser investigative requirements, which is granted on a temporary basis, pending the completion of the full investigative requirements.

1-242 Internal Security. This refers to the prevention of action against U.S. resources, industries, and institutions and the protection of life and property in the event of a domestic emergency by the employment of all measures, in peace or war, other than military defense.

1-243 Locked Entrance. A locked entrance is an entrance to a Closed or Restricted Area which is kept closed and locked at all times except when temporarily unlocked and opened under supervision for the purpose of passing material or authorized personnel into or out of the area.

1-244 Long Title. The full title or name assigned to a publication, an item of equipment, or device is the long title.

1-245 Material. Material refers to a product or substance on, or in which, information is embodied.

1-246 Multiple Facility Organization (MFO). A legal entity (single proprietorship, partnership, association, trust, or corporation) which is composed of two more facilities (see paragraph 1-229) is a MFO.

1-247 National of the United States. A national of the U.S. is:

- a. a citizen of the U.S.; or
- b. a person who, although not a citizen of the U.S., owes permanent allegiance to the U.S. 10/.

*

1-248 NATO Classified Information. The term "NATO classified information," embraces all classified information, military, political, and economic that is circulated within and by NATO whether such information originates in the organization itself or is received from members nations or from other international organizations.

1-249 Need-to-Know. This is a determination made by the possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to (see paragraph 1-201), knowledge of, or possession of the classified information in order to perform tasks or services essential to the fulfillment of a classified contract or program approved by a UA.

1-250 Negotiator. Any employee, in addition to the OODEPs, who requires access to classified information during the negotiation of a contract or the preparation of a bid or quotation pertaining to a prime or subcontract is a negotiator. (This category may include, but is not limited to, accountants, stenographers, clerks, engineers, draftsmen, and production personnel.)

1-251 Officers (Corporation, Association, or Other Types of Business or Educational Institution). This definition includes persons in positions established as officers in the articles of incorporation or bylaws of the organization, including all principal officers; that is, those persons occupying positions normally identified as president, senior vice president, secretary, treasurer, and those persons occupying similar positions. In unusual cases, the determination of principal officer status may require a careful analysis of an individual's assigned duties, responsibilities, and authority as officially recorded by the organization.

1-252 Official Information. Information which is owned by, produced for or by, or is subject to the control of the U.S. Government is official information.

10/ See 8 U.S.C. (Section 1101(a)(22)), reference (n). 8 U.S.C. § 1401, subsection (a) lists in paragraphs (1) through (7) categories of persons born in and outside the U.S. or its possessions who may qualify as nationals of the U.S. Where doubt exists as to whether or not a person can qualify as a national of the U.S., this subsection should be consulted.

*

1-252a. Operations Security (OPSEC). The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities. Section X of this regulation contains a detailed discussion of OPSEC and UA responsibilities pertaining thereto. See JCS Pub 18 for further terms and definitions related to OPSEC. *

1-252b. OPSEC Indicators. Actions or information (classified or unclassified) obtainable by an adversary, that would allow the adversary to develop or confirm assumptions, estimates and facts about United States intentions, military capabilities, plans, or programs, thereby compromising essential secrecy. *

1-252.1 Parent. A parent firm is a corporation which can control another corporation (subsidiary) by ownership of a majority of its stock. The control may exist by direct stock ownership of an immediate subsidiary or by indirect ownership through one or more intermediate levels of subsidiaries.

1-253 Possessions. Possessions include the Virgin Islands, Guam, American Samoa, and the Guano Islands with Swains Island, Howland Island, Baker Island, Jarvis Island, Midway Islands, Kingman Reef, Johnston Island, Sand Island, Navassa Island, Swan Islands, and Wake Island.

1-253.1 Principal Management Facility (PMF). The PMF is a cleared facility of a MFO which reports directly to the HOF, and whose principal management official has been delegated the responsibility to administer the contractor's industrial security program, within a defined geographical or functional area.

1-254 Reference Material. This refers to documentary material over which the UA does not have classification jurisdiction and did not have classification jurisdiction at the time such material was originated. Much material made available to the contractors by the DTIC and other secondary distribution agencies is reference material as thus defined.

1-255 Regrade. To regrade is to assign a higher or lower security classification to an item of classified material.

1-256 Representatives of a Foreign Interest (RFI). This refers to citizens or nationals of the U.S. or immigrant aliens who, in their individual capacity, or on behalf of a corporation (whether as a corporate officer or official or as a corporate employee who is personally involved with the foreign entity), are acting as representatives, officials, agents, or employees of a foreign government, firm, corporation, or person. However, a U.S. citizen or national who has been appointed by his or her U.S. employer to be a representative in the management of a foreign subsidiary (for example, a foreign firm in which the U.S. firm has ownership of at least 51% of the voting stock) will not be considered a RFI, solely because of this employment, provided the appointing employer is his or her principal employer and is a firm that possesses or is in process for a FCL.

1-257 Restricted Area. This is a controlled area established to safeguard classified material which, because of its size or nature, cannot be adequately protected during working hours by the safeguards prescribed in paragraph 16, ISM, but which is capable of being stored during non-working hours in accordance with paragraph 14, ISM (see section IV, ISM).

1-258 RESTRICTED DATA. All data (information) concerning: (i) design, manufacture, or utilization of atomic weapons; (ii) the production of special nuclear material; or (iii) the use of special nuclear material in the production of energy, but not to include data declassified or removed from the RESTRICTED DATA category pursuant to Section 142 of the Atomic Energy Act (see § 11y, Atomic Energy Act of 1954, reference (o), and paragraph 1-233, ISR, on FORMERLY RESTRICTED DATA).

1-259 SECRET. "SECRET" is the designation that shall be applied only to information or material, which the unauthorized disclosure of 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.

1-260 Security. Security refers to the safeguarding of information classified TOP SECRET, SECRET, or CONFIDENTIAL against unlawful or unauthorized dissemination, duplication, or observation.

1-261 Security Cognizance. This is the responsibility for acting for UA's in the discharge of industrial security responsibilities described in this regulation.

1-261.1 SENSITIVE COMPARTMENTED INFORMATION. This term includes all information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. The term does not include RESTRICTED DATA as defined in Section 22, Public Law 83-703, Atomic Energy Act of 1954, reference (o).

1-262 Short Title. This is an identifying combination of letters and numbers assigned to a publication or equipment for purposes of brevity.

1-263 Special Access Program. This refers to any program imposing "need-to-know" or access controls beyond those normally provided for access to CONFIDENTIAL, SECRET, or TOP SECRET information. Such a program includes, but is not limited to, special clearance, adjudication, or investigative requirements; material dissemination restrictions; or special lists of persons determined to have a "need-to-know."

1-264 Subsidiary. A subsidiary is a corporation which is controlled by another corporation (parent) by reason of the latter corporation's ownership of at least a majority (over 50%) of the capital stock. A subsidiary is a legal entity and shall be processed separately for a FCL.

1-265 Telecommunications. The transmission, communication, or processing of information, including the preparation of such information thereof, by electrical, electromagnetic, electromechanical, or electro-optical means.

1-265.1 TEMPEST. TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations (see paragraph 1-217.1).

1-266 Time Resource Sharing. For the purpose of this regulation, the term applies to the concurrent use of an ADP system by one or more users. The term includes the functional characteristics of an ADP system which allow simultaneous or apparently simultaneous access to all or part of the ADP system by more than one user or the acceptance and processing of more than one computer program of instructions. The term encompasses the characteristics of time-sharing, multiprocessing, multiprogramming, or combinations of these functional capabilities in any form.

1-267 TOP SECRET. "TOP SECRET" is the designation that shall be applied only to information or material, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the U.S. or its allies, disruption of foreign relations vitally affecting the national security, the compromise of vital material defense plans or complex cryptologic and communications intelligence systems, the revelation of sensitive intelligence operations, and the disclosure of scientific and technological developments vital to national security.

1-268 Transmission Security. Transmission security is that component of security which result from all measures designed to protect communication transmissions from interception and traffic analysis.

1-269 Trust Territory. This definition applies only to the trust territory of the Pacific Islands which the U.S. administers under the terms of a trusteeship agreement concluded between this government and the Security Council of the United Nations pursuant to authority granted by Joint Resolution of Congress, July 18, 1947 (61 Statute. 397, Title 48 U.S.C., § 1681) (reference (p)). According to this agreement, the U.S. has "full power of administration, legislation, and jurisdiction" over the territory; this government, however, does not claim "sovereignty." Three major archipelagoes make up the

trust territory: Carolines (including the Palau Islands), Marshalls, and Marianas (excluding Guam).

1-270 Unauthorized Person. Any person not authorized to have access to specific classified information in accordance with the provisions of the ISM and this regulation is an unauthorized person.

1-271 United States. This is the 50 states and District of Columbia.

1-272 Upgrade. To upgrade is to determine that certain classified information requires, in the interests of national security, a higher degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such a higher degree.

1-273 User Agencies (UA's). This term refers to the OSD (including all boards, councils, staffs, and commands), DoD agencies, and Departments of Army, Navy, and Air Force (including all of their activities); National Aeronautics and Space Administration; General Services Administration; Small Business Administration; National Science Foundation; Environmental Protection Agency; and the Departments of State, Commerce, Treasury, Transportation, Interior, Agriculture, Labor, and Justice; U.S. Arms Control and Disarmament Agency, Federal Emergency Management Agency, the Federal Reserve System; General Accounting Office; and the U.S. Information Agency. *
*
*

Part 3. SECURITY COGNIZANCE

1-300 Policy.

a. Administration of the DoD Industrial Security Program is assigned to the Director, DIS. Security cognizance authority is delegated to the Regional Directors of Industrial Security for all contractor facilities physically located within the geographic boundaries of their respective jurisdictions (see appendix B). The Regional Director of Industrial Security shall perform all cognizant security functions prescribed in this regulation and the ISM on behalf of all UA's unless the provisions of paragraphs 1-108 or 1-115 apply, in which case the Commander or Head of the UA installation shall perform certain security actions.

b. All relationships between the UA and the contractor on industrial security matters shall be handled through or in coordination with the CSO except those matters specifically set forth in this regulation and the ISM as responsibilities of the UA contracting activity.

c. The assumption of industrial security cognizance by the Director of Industrial Security will not relieve any UA of the responsibility for protecting and safeguarding its classified material incident to its classified contracts with the facility, or from visiting the facility to review the security aspects of such contracts. However, visits by a representative of a UA to a facility to review security aspects of a contract shall be coordinated with the CSO prior to such visits. Any deviation from the requirements of the ISM or special security requirements under the contract, which may be noted

during the visit shall be referred promptly to the CSO, with suggested corrective action or additional security requirements to be levied on the contractor. The CSO shall take appropriate action regarding these matters, and, if requested, shall notify the UA of the corrective action taken by the contractor.

d. International operations are the responsibility of the Deputy Director (Industrial Security), HQ DIS.

e. PCL actions are the responsibility of the Director, DISCO.

f. With respect to commercial carriers, the authority for security cognizance has been delegated to each CSO for those elements of carriers physically located within the geographic boundaries of each region. All relationships between the government and commercial carriers on safeguarding SECRET controlled shipments shall be handled through or in coordination with the CSO. Commercial carriers which have been assigned to one of the CSO's for security cognizance shall be notified in writing of this action.

g. With the exception of candidate material (CM) (CONFIDENTIAL or SECRET category), when an escort is used, the company furnishing the transportation service (ship, rail, air, or truck) is not required to have a FCL. An escort shall always be used when ship or rail transportation is involved. Consequently, ship and railroad companies will not be issued a FCL. When a shipment by truck is contemplated for classified CM (CONFIDENTIAL or SECRET), the contracting officer will issue specific shipping instructions, requiring a driver holding a final SECRET clearance in addition to the military escort normally provided for such shipments..

h. The CSO of the HOF of a carrier is responsible for maintaining a central master file containing copies of pertinent reports and correspondence concerning all violations, major deficiencies, unsatisfactory conditions, and major problem areas in the carrier's system, regardless of the geographical area of the terminal involved. It is the responsibility of the CSO of the terminals to assure that copies of such pertinent reports and correspondence are furnished the CSO of the HOF.

1-301 Functions of a Cognizant Security Office. Procedures set forth in this regulation prescribe the functions and responsibilities of the CSO.

1-302 Notification of Security Assignment. The management of each facility which has been assigned to a CSO for security cognizance shall be notified in writing of this assignment when a FCL action is to be initiated for the facility.

1-303 Procedural Changes. All questions of interpretation with respect to procedures or methods prescribed in the ISM or this regulation shall be answered by the CSO, except that interpretations of security classification guidance, procedures, or methods shall be provided by the contracting officer of the UA, or his or her designated representative. For facilities or contractor activities located on a UA installation (see paragraphs 1-108 and 1-115), requests from the contractor for interpretations of the requirements of the ISM shall be forwarded to the CSO through the Commander or Head of the installation. In all instances where this regulation or the ISM requires that

management of a facility be advised regarding changed industrial security procedures or methods, the CSO shall so advise management.

1-304 Defensive Security Briefing.

a. When a report is received from a contractor, the CSO, or UA, in accordance with paragraph 6b(9), ISM, that a cleared employee or Type A Consultant has traveled to or through a Designated 11/ country, or attended * an international scientific, technical, engineering, or other professional meeting when a representative of a Designated country participated or was in attendance (hereinafter called foreign travel), the DISCO shall review the records available in the PSCF, in light of the employee's travel. If the PSCF records indicate a background investigation (BI) or expanded national agency check (ENAC) or any investigative coverage other than a satisfactory national agency check (NAC), the investigative file shall be obtained and reviewed. If the PSCF records indicate that the only investigation conducted in the case is a satisfactory NAC, it will not be necessary to obtain the investigative file. However, where possible, the "Department of Defense Personnel Security Questionnaire (Industrial-NAC)" (DD Form 48) or "Department of Defense Personnel Security Questionnaire (Industrial)" (DD Form 49) submitted by the individual in connection with the application for clearance shall be reviewed.

(1) The DISCO shall request additional investigation in those cases in which the employee's report of intended foreign travel discloses discrepancies between this report and information previously furnished or developed by the government. For example, where the "Department of Defense Personnel Security Questionnaire (Industrial-NAC)" or "Department of Defense Personnel Security Questionnaire (Industrial)" submitted in connection with the clearance application indicates the individual has no relatives residing in Designated countries, and yet the purpose of the intended foreign travel is to visit a relative in a Communist country, it is necessary to determine through investigation whether the original clearance application was fraudulent and if the case currently presents a hostage problem as discussed in paragraph 2-305. Moreover, in those cases where the investigation conducted in connection with the clearance application raised serious questions concerning such things as the individual's suitability, trustworthiness, or national allegiance, it may be necessary to update the investigation and reevaluate the case in light of this new element of foreign travel which brings the individual in direct contact with or to the attention of officials or representatives of a Designated country.

11/ Designated countries (those countries whose policies are inimical to * U.S. interests) are: Iran, Afghanistan, Angola, Ethiopia, Iraq, Nicaragua, South Yemen, Syria, Libya, Albania, Bulgaria, Kampuchea (formerly Cambodia), People's Republic of China (including Tibet), * Cuba, Czechoslovakia, North Korea, German Democratic Republic (GDR) (East Germany, including the Soviet Sector of Berlin), Hungary, Laos, Mongolian People's Republic (Outer Mongolia), Poland, Rumania, Union of Soviet Socialist Republics (USSR) (including Estonia, Latvia, Lithuania, and all the other constituent republics, Kurile Islands and South Sakhalin (Karafuto)), Vietnam, and Yugoslavia.

(2) The report of the employee's foreign travel furnished by the contractor pursuant to paragraph 6b(9), ISM, shall be recorded in the PSCF. While most cases do not fall within the purview of paragraph a above, and do not require additional investigation, it may be necessary because of the number or frequency of such visits to initiate additional investigation to determine if there is any security significance to the foreign travel in light of the individual's current PCL status.

(3) Where results of the additional investigation initiated pursuant to paragraphs 1 or 2 above indicate that the individual's continued access to classified information is not clearly consistent with the national interest, action shall be initiated in accordance with paragraph 2-320.

b. When a report is received from the contractor in accordance with paragraph 6a(19), ISM, that a Designated country representative(s) or national(s) will visit the facility, the CSO shall immediately follow up with the contractor by telephone or visit as appropriate to ensure that adequate safeguards have been established for controlling such visitors, especially when the visit is to be over an extended period of time. The contractor shall also be reminded to strictly apply the guidance in appendix VII, ISM, and to obtain the contractor's assistance in identifying any security problems involved in such visits. Further, during the course of the next recurring inspection the contractor's procedures for conducting the briefings required by appendix VII, ISM, shall be reviewed and verification made that the briefings required by paragraph 5u, ISM, were accomplished. *

1-305 Responsibility for the Security of SENSITIVE COMPARTMENTED INFORMATION Contracts.

a. Where a procurement activity awards a SENSITIVE COMPARTMENTED INFORMATION contract for the National Security Agency (NSA), exclusive security responsibility remains with NSA and that agency shall prescribe the security requirements for the contract. The NSA will process access authorizations for SENSITIVE COMPARTMENTED INFORMATION for contractor employees used on such contracts. The CSO and contracting activity are relieved of security responsibilities pertaining to such SENSITIVE COMPARTMENTED INFORMATION contracts.

b. Where a SENSITIVE COMPARTMENTED INFORMATION contract is awarded by and for a UA other than NSA, the UA will designate an activity which shall have exclusive security responsibility for, and shall prescribe the security requirements for the contract. The designated activity will process access authorizations for SENSITIVE COMPARTMENTED INFORMATION for contractor employees used on such contracts. The CSO and the contracting officer, except as may be specifically delegated by the designated activity, are relieved of security responsibilities pertaining to such SENSITIVE COMPARTMENTED INFORMATION contract.

c. When a SENSITIVE COMPARTMENTED INFORMATION contract is awarded, item 15 of the "DoD Contract Security Classification Specification" (DD Form

254), shall specify the activity which has exclusive security responsibility for this contract.

d. Access authorizations for SENSITIVE COMPARTMENTED INFORMATION will be processed in the following manner.

(1) The contracting office shall instruct the contractor to submit clearance applications to the appropriate activity of NSA or the UA activity other than NSA.

(2) The NSA, or where appropriate, the UA activity with security responsibility will provide the contractor appropriate notification of the access authorization for SENSITIVE COMPARTMENTED INFORMATION.

1-306 Operational Responsibility for NSA COMSEC Account. Where a procurement activity awards a COMSEC contract for the NSA and a COMSEC account is required, exclusive operational responsibility for the account remains with NSA. The NSA COR will establish the account in accordance with paragraph 1-504. The NSA COR or its designated representative shall ensure that the custodians are instructed on all operational aspects regarding control, accountability, and handling of accountable COMSEC material. It will conduct audits annually, or more frequently when required, to ensure custodians are following prescribed procedures in the operations of the COMSEC account. The procurement activity is relieved of operational responsibility pertaining to the COMSEC account. The CSO will be guided by DoD 5220.22-S-1 (reference (q)) and by instructions furnished to the contractor by NSA COR, prescribing the type of COMSEC material, records, reports, and procedures to be utilized by the custodian in maintaining control and accountability of the COMSEC material.

Part 4. SPONSORSHIP OF MEETINGS

1-400 Application. The following provisions apply to a conference, seminar, symposium, exhibit, or convention at which classified information is disclosed and which is conducted by a DoD Component, a cleared DoD contractor, or by an association, institute, or society whose membership consists of DoD contractors, contractor employees, or DoD personnel. These provisions do not apply to meetings related to a specific contract or project, including preproposal or preaward meetings, and postaward briefings conducted by the DoD contracting activity. Also, meetings conducted by a cleared contractor(s) and attended by cleared contractor personnel directly involved in the performance of a contract or project are excluded from the provisions of this part. Provisions of paragraph 1-408 apply to meetings described in paragraph 5q(3) and (4), ISM. Sponsorship of meetings by a UA other than DoD will be in accordance with the procedures of that agency.

1-401 General Policy. All meetings conducted within the scope of this part must be sponsored for security by a DoD Component. The Head of a DoD Component, or designee, having a significant interest in the subject matter, may sponsor a meeting for security after determining that:

a. the conduct of classified sessions of the meeting is in the best interests of the national security,

b. the use of conventional channels for dissemination of classified scientific and technical information would not accomplish the purpose of the meeting,

c. adequate security measures and access procedures have been developed and will be carried out, and

d. the location selected for the classified sessions of the meeting facilitates the proper control and dissemination of classified information and adequate facilities are available for its storage and protection.

1-402 Requests for Sponsorship. When requested by an association, institute, or society whose membership is comprised primarily of contractors cleared by DoD, contractor employees, or DoD personnel, a DoD Component may sponsor a meeting for security purpose, provided the DoD Component or a designated cleared contractor undertakes overall security responsibility and security administration.

1-403 Guides for Sponsorship. Sponsorship for security purposes shall be by a single government activity having a principal interest in the subject matter. Acceptance of sponsorship for security purposes by the department or agency does not relieve any other activity from responsibility for authorizing or prohibiting the release or dissemination of information under its jurisdiction. When appropriate, the department or agency sponsoring the meeting for security purposes may request other DoD activities to provide such assistance, facilities, or support as may be justified in the interest of economy, efficiency, and security. Sponsorship for security purposes shall be granted only for a meeting conducted by a cleared contractor. However, a meeting conducted by an association, institute, or society whose membership consists of cleared contractors may be sponsored for security purposes, provided a cleared contractor is designated and accepts responsibility on behalf of the association, institute, or society for ensuring the security measures and procedures at the meeting.

a. Sponsorship normally shall be granted only for a meeting conducted by a cleared contractor. However, a meeting conducted by an association, society, or group whose membership consists primarily of cleared contractors may be sponsored provided a cleared contractor is designated and accepts responsibility on behalf of the association, society, or group for providing the security measures and procedures at the meeting.

b. Meetings shall be sponsored only when there is assurance that adequate security measures have been planned and will be conscientiously executed. Prior to accepting sponsorship, a determination shall be made that

the location selected for the meeting site ensures adequate safeguarding and control of dissemination of classified information 12/. *

1-404 Location of Meetings. The activity sponsoring the meeting for security is responsible for evaluating and approving the location proposed for the meeting.

a. A meeting at which TOP SECRET or SECRET information is to be disclosed shall be held only at a U.S. Government or cleared contractor facility; that is, a facility in a fixed location where adequate measures for safeguarding classified information can be imposed. Under this criteria, the proposed meeting site would have to be on a government installation or at a cleared contractor facility. In either case the meeting must be held in an area of the government installation or contractor facility that can be secured. An auditorium, assembly hall, or gymnasium which is used primarily for campus activities and public gatherings cannot be secured and shall not be approved for a classified meeting at which TOP SECRET or SECRET information would be disclosed, even though it is located on the campus of a university or college, portions of which are a cleared facility.

b. A meeting at which information classified no higher than CONFIDENTIAL is to be disclosed normally shall be held at a U.S. Government installation or at a cleared contractor facility. However, the Head of the DoD Component sponsoring the meeting for security may approve the use of another location for such a meeting, provided suitable facilities are not available at a government installation or cleared contractor facility, and the sponsoring activity determines that adequate security can be maintained at the proposed location. The authority to approve a location other than a U.S. Government installation or cleared contractor facility may not be delegated, except that a Secretary of a Military Department may delegate his or her authority to an Assistant Secretary of that Department. A contractor's request to use a location other than a cleared contractor's facility or a U.S. Government installation shall be in compliance with paragraph 9c(2), ISM.

1-405 Security Procedures. The sponsoring activity is responsible for reviewing and approving the security measures and procedures developed by the contractor, for ensuring the security of the classified information, and for supervising and assisting in the development and application of those procedures. The security measures shall include adequate arrangements for the following.

a. Strictly limiting attendance at a classified meeting to authorized persons -- this shall include measures for determining that all persons on the approved list of attendees have been granted a security clearance equal to or higher than the category of information to be discussed, and have duties requiring such access. For contractor personnel, the certification of security clearance and need-to-know shall be accomplished as provided in paragraph 1-409.

12/ Sponsorship of meetings by a UA other than the DoD will be in accordance * with the procedures of that agency.

b. Reviewing and approving all announcements and invitations related to the meeting and lists of attendees pertaining thereto -- announcements and invitations shall be unclassified and shall include the specific name of the sponsoring activity and the date of approval.

(1) Notices and announcements of meetings, whether classified, unclassified, or mixed, and not amounting to invitations to attend, may be published publicly, provided classified information is not included in such notices or announcements.

(2) In the case of a classified meeting, invitations to attend, whether on an individual or class basis, shall not be sent to a person known to be a national from, or a representative of, a Communist country.

c. Safeguarding and controlling the distribution of notes, minutes, summaries, recordings, proceedings, and reports on the classified portions of the meeting -- such material normally shall be sent only to those approved for attendance at the classified sessions. However, the sponsoring activity may also authorize distribution to others who are determined to be eligible for and who require access to the classified information involved. In any event, the material shall be sent only to a government activity or cleared contractor facility and marked for the attention of the intended recipient, as provided in paragraph 17, ISM.

d. Security measures shall include notifying each person who presents or discloses classified information at the meeting of the security limitations on disclosures for such reasons as the level of clearance or need-to-know of members of the audience, or other limitations required by the National Disclosure Policy of the government or directives of UA's.

e. Ensuring the physical security of the meeting site and the area used for classified sessions or displays -- this shall include provisions for guards, entrance controls, personnel identification, storage facilities, and adequate security against unauthorized access to, or illicit acquisition of, the classified information. Classified sessions of mixed meetings, that is, those having both classified and unclassified sessions, shall be held at places geographically separated from the place where unclassified sessions are held.

f. Security measures shall include ensuring that attendance at a meeting or session at which classified information is to be disclosed is limited to persons whose names appear on the access list approved by the sponsor, and who present proper identification.

g. Security measures shall include ensuring that individuals making oral presentations at meetings provide classification guidance sufficient to enable attendees to identify what information is classified or unclassified, and if classified, at what category or categories of classification.

h. Security measures shall also include reviewing the minutes, summaries, recording, proceedings, and reports of the meeting to eliminate any classified information or to limit distribution in accordance with paragraph c above.

1-406 Controlling Disclosures. The sponsoring activity shall require a contractor desiring to disclose classified information to furnish written approval from the contracting officer concerned prior to the meeting. The sponsoring activity shall:

a. maintain a central record of disclosure authorizations granted for contractor's presentations and displays,

b. require the contractor to furnish a copy of each classified presentation as actually made at the meeting, and

c. monitor the meeting to assure that classified information is disclosed only to the extent authorized.

1-407 Attendance by Foreign Nationals and Representatives of a Foreign Interest 13/. *

a. As a general rule, a DoD Component will not agree to sponsor a meeting for security if foreign nationals or representatives of foreign governments are to be in attendance at sessions of such meetings which involve the disclosure of classified military information. As an exception to this general rule representatives of, and nationals from, foreign countries, other than Designated countries, may attend classified sessions only when the Head of a DoD Component sponsoring the meeting for security, or a designee, determines that such attendance is consistent with National Disclosure Policy (NDP-1) (reference (r)) and specifically authorizes it in writing.

b. Representatives of, and nationals from, other than Designated countries may attend unclassified sessions without specific authorization, provided the disclosure of unclassified technical data, which is governed by the Export Administration Act of 1969 (reference (s)), as amended, as administered by the Secretary of Commerce, and Section 38 of the Arms Export Control Act (reference (t)) as administered by the Secretary of State through the ITAR (reference (i)), are complied with.

c. Representatives of, and nationals from, Designated countries may not attend a classified session under any circumstances. However, they may attend unclassified sessions when the Head of the DoD Component security sponsoring the meeting approves individually and in writing, on a name basis, such attendance when clearly justified as being in the national interest. This authority may not be delegated. When the attendance of such individuals at an unclassified session or presentation of a meeting is requested by the contractor, the activity sponsoring for security will forward the request through channels, recommending approval or disapproval. Such requests shall comply with paragraph 9b of the ISM, and will show how approval will further reci-

13/ A person granted a reciprocal clearance or a RFI cleared for access to classified information under the DoD Industrial Security Program is not subject to the limitations of paragraph 1-407, provided the information is releasable under National Disclosure Policy. However, persons granted reciprocal clearances are subject to the access limitations prescribed in paragraphs 2-322 and 2-324. *

procuity for attendance of U.S. personnel at similar meetings within Designated countries. No invitation shall be tendered, either formally or informally, by or on behalf of the contractor, to a foreign national or representative of a Designated country or to his or her government or firm until his or her attendance has been approved.

d. The DoD Component which approves a request for attendance by a national from, or representative of, a Designated country at unclassified sessions of a meeting shall provide the Soviet and Eastern European Exchange Staff, Department of State, New State Building, Washington, D.C. 20520, the names of the proposed invitees, date of attendance, the location of the meeting, the subject matter to be discussed, and titles of scientific, technical, or other papers to be presented. The admissibility to the U.S. of these proposed invitees must be determined prior to the issuance of the actual invitation, if they have not already been admitted with a visa.

e. The sponsoring activity shall:

(1) advise the contractor of the approval or disapproval of the attendance of foreign nationals or RFI's at the meeting;

(2) ensure that foreign nationals or representatives of a foreign interest other than Designated countries are excluded from all classified sessions, presentations, and displays except those which they have specifically been authorized to attend; and

(3) ensure that foreign nationals or representatives of Designated countries are excluded without exception from all classified sessions, presentations, and displays and from all unclassified portions of sponsored meetings, except those which they have specifically been authorized to attend.

1-408 Disclosure Authorizations. The release of classified information by government representatives participating in contractor-conducted meetings shall be authorized in accordance with pertinent directives of their individual departments or agencies. Contracting officer approval of proposed disclosures by contractors of classified information at contractor-conducted or government-conducted meetings shall be accomplished as follows.

a. Proposals from a contractor to disclose classified information at a meeting conducted under paragraphs 5q(3) or (4), ISM, shall be processed in accordance with the pertinent directives of the contracting activity having jurisdiction over the information involved.

b. If the proposed disclosure is approved, the contractor shall be notified in order that he or she, in turn, may advise the sponsoring activity.

1-409 Approval for Attendance at Classified Meetings. When a contracting officer or an official monitoring a UA program receives an application from a contractor for one or more of his or her employees to attend a classified meeting, he or she is required to determine the contractor's FCL, and need-to-know. The determination by the contracting officer or monitoring official of the FCL may be based on knowledge acquired through a current classified contractual relationship, program participation, or by verifying the FCL with

the PIC-CVA. The need-to-know determination can be made after reviewing the justification submitted by the contractor with the application. The general criterion for this determination will be whether, in the interest of national security, the contractor requires access to the classified information to be disclosed at the meeting in order to perform tasks or services essential to the fulfillment of a classified contract or program. After the FCL has been determined, the contractor's certification as to the PCL status and need-to-know of the employees who will attend the meeting shall be accepted. The contracting officer or monitoring official, after completing his or her required actions, provided that the contractor has certified that the employee is cleared at the appropriate level and has the need-to-know, will forward the contractor's application and certification to the sponsoring activity, indicating that the FCL has been verified and the need-to-know has been determined. *

1-410 Notification. DoD Components sponsoring meetings for security shall notify the DUSD(P) ATTN: Director for Security Plans and Programs (DSP&P), of each meeting's subject matter or title, location, and date. This notification should be given at the time the DoD Component agrees to sponsor for security and can be accomplished by providing a copy of the letter reflecting this agreement. When reports of loss or compromise of classified information as a result of such a meeting are prepared in accordance with section V of this regulation, the DUSD(P) ATTN: DSP&P, shall be notified by copies of such reports.

Part 5. PROCEDURES PERTAINING TO COMSEC INFORMATION

1-500 Application. The procedures in this regulation pertaining to COMSEC information shall apply to, and shall govern, the industrial security relationship between UA's and contractors under one or a combination of the following conditions:

- a. when the contractor requires the use of CRYPTOSYSTEMS in the performance of his or her contract;
- b. when the contractor is required to install, maintain, or operate CRYPTO equipment for the U.S. Government; or
- c. when the contractor is required to accomplish research, development, or production of CRYPTOSYSTEMS, CRYPTO equipment, or related COMSEC material.

1-501 Instructions Concerning COMSEC Material.

- a. Requirements for the safeguarding of COMSEC material in the hands of industry are established in reference (q).
- b. Distribution of reference (q) will be made by the CSO's and shall be limited to UA's and contractors meeting the conditions established in paragraph 1-500.

1-502 Release of COMSEC Information and Material to U.S. Contractors. Basic policy and procedures pertaining to the release of COMSEC information and material to U.S. contractors and to the use of COMSEC material by U.S. contractors are set forth in detail in National Communications Security Committee publication NCSC-2, "National Policy on Release of Communications Security Information to U.S. Contractors and Other U.S. Nongovernmental Sources," reference (u). Additional guidance is contained in appropriate DoD and UA instructions. Any request for a waiver from the provisions of references (q) or (u) shall be submitted to the Director, DIS, ATTN: Deputy Director (Industrial Security).

a. Use of COMSEC Material by Contractors.

(1) Contractors engaged in work on classified contracts may be authorized and should be encouraged to use certain CRYPTOSYSTEMS for the encryption of classified or unclassified, national security-related information. Use of a CRYPTOSYSTEM may be authorized for the encryption of classified or unclassified, national security-related communications between contractors and the U.S. Government, between contractors, between various facilities of a contractor, and between contractors and subcontractors. A CRYPTOSYSTEM when approved, may be used by the contractor for the transmission of information classified no higher than that approved for the CRYPTOSYSTEM. Use is not limited to the contract for which originally approved.

(2) The contractor shall submit a request for approval of the use of a CRYPTOSYSTEM to the contracting officer concerned. In turn, the request shall be processed in accordance with appropriate contracting activity instructions.

(3) When use of a CRYPTOSYSTEM is authorized, the contracting activity shall:

(a) specify the levels of classified information which may be encrypted; and

(b) ensure, prior to issuance of the CRYPTOSYSTEM, that:

1 procedures are established to provide for the physical safeguarding of COMSEC materials and for the secure and efficient operation of the CRYPTOSYSTEM; and

2 security clearances for the highest classification of information or material have been granted by the U.S. Government to all persons who may require access and that these persons have been given a COMSEC briefing.

b. Utilization of Contractor Personnel in Government COMSEC Operations. From the standpoint of security and control of operations during both normal and emergency conditions, the installation, maintenance, and operation of U.S. Government secure telecommunications systems normally should be performed by appropriately cleared U.S. citizens who are military personnel or civilian employees of the government.

(1) In those cases where the installation, maintenance, and operation of secure telecommunications systems by contractor personnel is considered in the best interest of the government, Heads of UA's may authorize the utilization of U.S. contractor personnel to perform these functions. The National Communications Security Committee (formerly USCSB) shall be advised of each instance where contractor personnel are utilized and of their terminations of such employment.

(2) When the utilization of contractor personnel in government COMSEC operations has been authorized, the contracting UA shall ensure that such persons have been cleared by the government at the appropriate level.

c. Utilization of Contractor to Accomplish Research, Development, or Production of COMSEC Information or Material. When in the best interests of the government, Heads of UA's may provide COMSEC material or information to a contractor for research, development, production, and testing of CRYPTO equipment, or of communications equipment interfacing with CRYPTO equipment, when such work is being undertaken on behalf of the government.

1-503 Subcontracting COMSEC Work.

a. Subcontracts requiring the disclosure of classified COMSEC information will be awarded only upon the written approval of the contracting officer of the prime contract. Prior to the approval of the subcontract, the contracting officer shall assure that the proposed subcontractor meets the security requirements of this regulation.

b. The subcontractor facility shall be inspected in accordance with paragraphs 4-103 and 4-107.

1-504 Establishing a COMSEC Account.

a. When COMSEC material which is accountable to a COR is to be provided or produced under a contract, the contracting officer shall inform the contractor that a COMSEC account must be established. In addition, the contracting officer shall notify the COR and the CSO that a COMSEC account shall be established. The contractor is then required to nominate a COMSEC *
custodian and an alternate COMSEC custodian, each of whom shall be a U.S. citizen.

b. The CSO shall forward the names of the persons nominated *
as FSO, COMSEC custodian, and an alternate to the COR, with a copy to the contracting activity, indicating that the persons have been cleared and have been given a COMSEC briefing in accordance with paragraphs 2-313 and 2-314.

c. The COR will then establish the COMSEC account and will include the applicable contract number on each letter of transmittal or transmittal voucher sent to the contractor.

d. An individual may be appointed as the COMSEC custodian for more than one account only when approved by each COR concerned.

1-505 Destruction and Disposition of COMSEC Material. The COR will provide directions to the contractor when accountable COMSEC material is to be destroyed. These directions may be provided in superseding editions of publications or by specific instructions.

1-506 Shipment of COMSEC Material Outside of a Facility.

a. The contracting activity shall provide the contractor approval of and instructions pertaining to the shipment of classified COMSEC material. Methods for shipment are contained in reference (q).

b. If contractor personnel are to act as couriers to transport TOP SECRET keying material marked "CRYPTO," they must be designated by the contracting activity. Such contractor personnel must be cleared for access to TOP SECRET material and must have been given a COMSEC briefing.

1-507 Unsolicited COMSEC Proposals. Any unsolicited COMSEC system, equipment, development, study, or proposal which is submitted by a contractor to a military department or an agency for consideration, shall be forwarded to the Assistant Director for Communications Security, National Security Agency, Fort George G. Meade, Maryland 20755, for evaluation and a determination as to whether or not it requires protection in the interest of national security.

Part 6. TRANSMISSION OF CLASSIFIED MATERIAL

1-600 Application. This part applies in those instances when, in accordance with paragraph 17, ISM, the contractor requires the approval of or instructions from the contracting activity for transmission of classified material outside the facility, and when CONFIDENTIAL material is transmitted to and from a contractor facility and a UA. *

1-601 Approved Methods of Transmission.

a. Approved methods for transmission of CONFIDENTIAL material outside a contractor facility are set forth in paragraph 17d, ISM. That paragraph provides, in part, that contractors shall transmit CONFIDENTIAL material to other contractor facilities by U.S. Express Mail, U.S. Certified, or Registered Mail, depending on the contractors' location.

b. UA's are not authorized to transmit CONFIDENTIAL material to a contractor facility by first class mail. Such material shall be transmitted only by U.S. Certified, U.S. Express or Registered Mail, in order to assure such transmission is received by an appropriately cleared employee of the contractor. *

c. In addition to the methods of transmission of classified material authorized in paragraph 17, ISM, contracting activities shall authorize additional methods when required in accordance with instructions contained in the

DAR and departmental or agency regulations. Further, when transmitting SECRET or CONFIDENTIAL material to an individual operating as a cleared facility or engaged as a Type B or Type C Consultant, or to any facility at which only one employee is assigned, it shall specify on the outer container: "TO BE OPENED BY ADDRESSEE ONLY." The outer container shall also be annotated: "POSTMASTER -- DO NOT FORWARD. IF UNDELIVERABLE TO ADDRESSEE, RETURN TO SENDER."

1-602 Contracting Officer Approval. Approval for or specific instruction to the contractor are required under the following conditions.

a. TOP SECRET material is to be transmitted outside a facility. The purpose of this requirement is to ensure that TOP SECRET information is not exposed to the inherent dangers of transmittal outside of the facility, unless essential to the performance of the contract.

b. The nature of the classified shipment does not lend itself to transmission by any of the methods specified in paragraph 17, ISM.

c. Use of Army, Navy, or Air Force postal facilities or Armed Forces Courier Service (ARFCOS) is required. However, such approval is not required provided that the contractor has previously received an authorization by virtue of his or her location on an overseas U.S. installation 14/. *

d. A CRYPTOSYSTEM is to be used for the transmission of SECRET and CONFIDENTIAL information. Once approved and installed, the CRYPTOSYSTEM may be used for the transmission of such information pertaining to other classified contracts without further approval of the contracting activity concerned. When an urgent requirement exists for transmitting a considerable amount of information to and from the facility, and other methods of transmission are inexpedient, the contractor may utilize the CRYPTOSYSTEM. TOP SECRET information shall not be transmitted over a CRYPTOSYSTEM without the specific prior approval of the contracting officer concerned.

14/ If the intended recipient is not authorized to receive classified material through Army Post Office (APO) channels, arrangements shall be made with a U.S. activity which is so authorized to receive and hold the classified material pending pickup by the intended recipient. *

e. For transmissions which are not within or between the U.S., Puerto Rico, or a U.S. possession or a trust territory, but which are necessary to serve a government purpose, the contractor shall request written authorization from the contracting officer when the classified material is to be transmitted by one of the following means:

(1) by use of a cleared contractor employee escort who has been designated by the contractor, provided the transmission does not cross international boundaries, is accomplished (begun and completed) during normal daytime duty hours of the same day, and is in accordance with the agreements in effect with the country concerned;

(2) by use of cleared U.S. military personnel or civil service employee designated to escort shipment -- foreign carriers shall not be utilized except when the escort has continuous physical control of the material being transmitted;

(3) by use of U.S. and Canadian registered mail and via a U.S. or Canadian government activity; or

(4) when the transmission of U.S. classified information to a foreign government is on a government-to-government basis (see paragraph 8-104).

On receipt of such request, the contracting activity shall verify the need for the shipment, determine that the procedures proposed by the contractor will provide a secure method of shipment, and assure that the shipment is destined for location where it can be stored under U.S. Government control or in the case of paragraph (4) above, it is under U.S. control until delivered to the representative of the foreign government. If the request meets the above requirements and is approved, the contracting activity shall so notify the contractor.

f. When shipment by truck is contemplated for classified CM (CONFIDENTIAL or SECRET), the contracting officer will issue specific shipping instructions, requiring a driver holding a final SECRET clearance in addition to the military escort normally provided for such shipments.

1-603 NATO Hand-carried Material. NATO regulations allow contractor employees to hand-carry NATO RESTRICTED, CONFIDENTIAL and SECRET material across international borders under certain conditions. A contractor may request the CSO to approve the use of an appropriately cleared and briefed employee for such purposes in accordance with paragraph 88d, ISM. The CSO, after determining that the criteria for exception to normal transmission procedures exists, may issue an appropriately stamped and signed NATO Courier Certificate. The necessary formats are illustrated at appendix G, ISR and paragraph B, section III, attachment 3 to enclosure 2, of the USSAN Instruction 1-69, and will be originals on official letterhead. The CSO should affix an official seal to the certificate. If a NATO seal is not available, an official DIS or company seal may be used. During the course of recurring inspections, the CSO shall confirm that employees who are issued NATO Courier Certificates have been properly briefed and the certificates accounted for. The CSO will account for all courier certificates produced by them. (a consecutive numbering system should be devised by each CSO for this purpose.)

Part 7. PROCEDURES PERTAINING TO COMMERCIAL CARRIERS

1-700 Application. This part establishes procedures for the qualification of commercial carriers by both MTMC and DIS for the movement of SECRET controlled shipments. It specifies the responsibilities of MTMC in the CONUS and of designated military Commanders in Alaska, Hawaii, Puerto Rico, and U.S. possessions and trust territories in their respective areas. It also specifies the responsibilities of CSO's assigned responsibility for assuring that commercial carriers can satisfactorily safeguard SECRET controlled shipments.

1-701 Instructions Concerning Commercial Carriers.

a. Requirements for the safeguarding of SECRET controlled shipments from consignor to consignee are established in the LSM and DoD 5220.22-C (reference (b)). These publications are distributed by the CSO's to cleared commercial carriers.

b. Appendix E reflects the areas serviced by MTMC and by military Commanders in Alaska, Hawaii, Puerto Rico, or a U.S. possession or trust territory.

c. Appendix F is a chart which identifies the primary functional responsibilities of the transportation officer (TO), MTMC, and the CSO's, with respect to the transmission of SECRET controlled shipments by commercial carrier.

d. Annex A of reference (b) incorporates a glossary of terms applicable to commercial carrier procedures.

e. Transportation officers should refer to the "Military Traffic Management Regulation," reference (y), for transportation policies and procedures.

1-702 Approval of Commercial Carriers. Commercial carriers shall be qualified by MTMC to move SECRET controlled shipments for the DoD, other UA's, and government contractors when the movement of material is within the CONUS, or by the designated military Commander when the movement of material is wholly within Alaska, Hawaii, Puerto Rico, or a U.S. possession or trust territory. In addition, they must be cleared by the CSO. Requests for qualification of initial and additional carriers shall be submitted through channels to the appropriate MTMC area headquarters or the designated military Commander (see appendix E) who shall maintain records of qualified commercial carriers and provide appropriate dissemination.

a. Qualification shall be based on the following.

(1) The requirement for the carrier's service has been established by a shipper.

(2) A determination has been made by MTMC or designated Commander that a qualified and cleared carrier is not available to perform the required service. In this connection, MTMC or the designated Commander shall

coordinate with the Deputy Director (Industrial Security), HQ DIS to ensure that a cleared carrier is not available.

(3) The carrier is authorized by law, regulatory body, or regulation to provide the required transportation service.

(4) A determination has been made by MTMC or designated Commander that the carrier is capable of, and authorized to, furnish PSS by applicable tariff, government tender, agreement, or contract provision, as required by paragraph b below.

(5) The carrier has been granted a SECRET FCL by the CSO.

b. The commercial carrier, by applicable tariff, government tender, agreement, or contract provision agrees to provide the following protective services for the movement of SECRET controlled shipments.

(1) The commercial carrier agrees to provide continuous person-to-person tally and signature of those persons providing en route protection while the shipment is in the carrier's custody; for air shipments, which are loaded into a compartment which is not accessible in flight, no receipt will be required from the flight crew or attendants of the carrier's aircraft on which shipments are being transported.

(2) The commercial carrier agrees to provide constant protection of the shipment at all times, between receipt from the consignor until delivery to consignee, by one or more cleared employees to prevent inspection, tampering, or pilferage. Observation of the shipment is not required during the period it is stored in the carrier's aircraft, in connection with flight, provided the shipment is loaded into a compartment aboard the aircraft which is not accessible to any unauthorized person.

(3) Closed and locked compartments or vehicles shall be used for shipment except when another method is authorized specifically by the shipper. In any event, exception shall not be granted for individual packages weighing less than 200 pounds gross.

(4) Shipments normally shall be afforded single-line service from point of origin to destination when such service is available. If time or distance does not permit movement through, the following security procedures will be observed.

(a) If the shipment remains in the transportation equipment, at least one of the cleared carrier custodians shall maintain constant protection to prevent access to shipment by unauthorized persons.

(b) If the material is unloaded from the vehicle, it shall be under the constant protection of a carrier custodian at the storage site or shall be placed in storage in a closed area, vault, or strongroom as defined in the ISM.

(c) In those cases in which the shipment is placed in storage en route, one of the cleared carrier custodians of the storage site shall execute the tally and signature service, and assume appropriate protection as prescribed.

c. The MTMC or the designated military Commander shall request the CSO of the commercial carrier's HOF to process the carrier and identified terminals for a FCL following completion of the actions prescribed in paragraphs a(1), (2), (3), and (4) above. Prior coordination with the Deputy Director (Industrial Security), HQ DIS will be made to determine the specific terminals to be processed for clearance. On receipt of a request for qualification, the CSO concerned shall complete the actions prescribed in section II, part 1 to permit an administrative determination to grant or deny a FCL to the carrier. During the initial survey, the CSO will assure that the contractor is aware that preparation of an acceptable SPP is a prerequisite to granting a FCL and that only those terminals listed by the HOF on the "Appendage to the Transportation Security Agreement" (DIS Form 1150) may be used for SECRET controlled shipments.

1-703 Responsibilities of Cognizant Security Offices. In addition to those actions prescribed in paragraph 1-702, CSO's assigned responsibility under paragraphs 1-300f and 1-300g of this section, shall be responsible for the following.

a. Inspect the HOF and the specific terminals of the carrier authorized to handle SECRET controlled shipments in accordance with the schedule in paragraph 4-103. The purpose of this inspection is to ensure that the carrier is complying with the terms of the "DoD Transportation Security Agreement" (DIS Form 1149), reference (b), and the carrier's SPP. Indications of noncompliance requiring more frequent or extensive types of inspection are not limited to those derived from inspections, but may be obtained from any reasonable source including complaints and prescribed reports submitted by any cleared contractor or government agency using this service.

b. Conduct appropriate inquiries into the circumstances involving delay in the movement of SECRET controlled shipments by commercial carriers, violation, or the possible loss of security due to misrouting, loss, tampering, or emergencies.

c. Advise the carrier's management of all deficiencies and of the requirement for corrective action in each case. Necessary follow-up inspections shall be performed by CSO's to determine the completion and effectiveness of corrective actions required of the carrier.

d. Ensure that the appropriate government investigative agency is advised of reports received by the CSO concerning existing or threatened espionage, sabotage, or subversive activities.

e. Advise carrier management concerning their obligations under the provisions of the DIS Form 1149, "Department of Defense Transportation Security Agreement," May 1983 (reference (dd)) and reference (b).

f. Determine the effectiveness of the carrier in protecting SECRET controlled shipments. If the carrier's performance is determined to be

unsatisfactory and cited discrepancies are not corrected within a reasonable period of time, the CSO shall take the action prescribed in paragraph 4-202. In order to provide for an adequate review of the effectiveness of a carrier's performance, all involved government or contractor activities shall furnish copies of all reports or incidents, investigations, inspections, surveys, or other documents which reflect unsatisfactory performance in the protection or movement of SECRET controlled shipments by a commercial carrier to the responsible CSO.

SECTION II. CLEARANCE PROCEDURES

Part 1. FACILITY SECURITY CLEARANCES AND DENIALS

2-100 Application. This part establishes the procedures for granting FCL's to contractors where access to classified information is required in order to perform tasks or services essential to the fulfillment of UA contracts, subcontracts, projects, or programs. This part also outlines the procedures for the denial, suspension, or revocation of FCL's.

2-101 Eligibility for Access. Classified information shall be furnished only to a contractor or subcontractor who holds a valid FCL at the appropriate level, has a need-to-know, and has the capability for safeguarding the information.

2-102 Facility Security Clearances.

a. A FCL is an administrative determination that the facility is eligible, from a security viewpoint, for access to classified information of the same or lower security category as the level of clearance being granted. FCL's will not be granted to contractor activities located outside the U.S., Puerto Rico, or a U.S. possession or trust territory. FCL's may be granted only to contractors organized and existing under the laws of the U.S. or Puerto Rico. Contractors organized and existing under the laws of a U.S. possession or trust territory may not be processed for or granted a clearance, except with the prior approval of the Deputy Director (Industrial Security), HQ DIS based on a case-by-case review of pertinent and current laws to determine the eligibility of the facility for the requested clearance. Facilities which are determined to be under FOCI are not eligible for a FCL (paragraph 2-201). Exceptions may be made when the foreign ownership or control emanates from a country with which the U.S. has entered formal reciprocal arrangements (see paragraph 2-117). A FCL (or interim FCL when so authorized) is required for prospective bidders or contractors prior to granting them access to classified information. Classified information which is of a higher category than the level of a FCL shall not be disclosed to that facility, its representatives, or employees, except to employees as authorized in paragraph 2-301a(2).

b. As an emergency measure and in order to avoid crucial delays in precontract or contract negotiations, the award of contract, or the performance on a contract, an interim FCL based on lesser investigative requirements may be granted on a temporary basis, pending the completion of the full investigative requirements. A UA when requesting the CSO to initiate interim FCL action, shall submit the reasons for such action at the time the clearance is requested, indicate the effect that any crucial delays will have on its precontract or contract negotiations, contract award, or contract performance, and state the level of FCL requested. The CSO shall comply with the request of the UA to initiate a FCL action, and will simultaneously take the action to effect an interim FCL. The authorization in connection with an interim TOP SECRET FCL will be made by the head of the UA or by his or her designated representative, and shall be furnished to the CSO which will process and grant the interim FCL. The CSO shall forward a copy of the authorization for interim FCL to DISCO. Actions as described in this subparagraph shall be clearly identified as an interim FCL.

2-103 Responsibility for Effecting a Facility Security Clearance. The CSO which has assumed cognizance of a facility shall be responsible for the processing of a FCL or interim FCL as may be required. Any prior industrial FCL actions that may have been accomplished prior to the issuance of this regulation, provided that these actions meet the standards prescribed in this regulation, shall not be duplicated, but shall be accepted by the CSO in effecting the FCL. Responsibility of the CSO for granting FCL's shall include performing the necessary DD Form 374 survey and requesting DISCO to process OODEPs as prescribed in paragraph 2-113 for a PCL at the same level as the FCL.

2-104 Types of Facilities. Generally, facilities are considered to be separate entities in accordance with the definition contained in paragraph 1-229. However, the following factors must also be taken into account where present.

a. When clearing a facility of a MFO, the HOF shall have a FCL of the same or higher level.

b. When a parent-subsidary relationship exists, the general rule is that the parent shall have a FCL of the same level or higher than the subsidiary. Paragraphs (1) and (2) below contain exceptions to this general rule.

(1) The parent may have a FCL of a lower level than that held by its subsidiary, if, by formal action of its board of directors or similar executive body, it is excluded from access to classified information held by the subsidiary company which is of a higher classification category than the parent company's FCL, and officers and directors of a subsidiary who hold similar positions in the excluded parent company furnish written certification to the CSO of each cleared subsidiary in accordance with paragraph 72a, ISM.

(2) The parent may be excluded from the requirement for a FCL if, by formal action of its board of directors or similar executive body, it is excluded from access to all classified information and delegates full authority to the subsidiary to act completely independently of the parent in all matters which involve or relate to the subsidiary's responsibility to safeguard classified information. In addition, the parent and the subsidiary shall execute a DD Form 441s prior to the granting of the FCL to the subsidiary. In this regard the CSO having jurisdiction in the area where the excluded parent is located shall be responsible for accomplishing the following actions.

(a) Request excluded parent to execute the DD Form 441s.

(b) Evaluate any element of FOCI which may be present within the excluded parent in the same manner as though the excluded parent were being processed for a FCL.

(c) Establish a facility case file on the excluded parent to record the action which is taken with regard to the FOCI question.

(d) Make an annual visit to the excluded parent to specifically determine if there have been any changes to the information previously provided on the DD Form 441s and to remind the excluded parent of its continuing responsibility to notify the CSO of any changes as they occur. Officers and

directors of a subsidiary who hold similar positions in the excluded parent company shall furnish certifications prescribed in paragraph 72a, ISM. The responsibility for obtaining such certifications is vested in the CSO having jurisdiction over the subsidiary. Subsidiaries of parent organizations which are under FOC1 are not eligible for clearance, except as provided for in paragraph 2-117. Whenever a parent becomes foreign owned, controlled, or influenced and the provisions of paragraph 2-117 are not applicable, the FCL of the subsidiary shall be terminated. Exclusion actions, as described in paragraphs (1) and (2) above, shall be made a matter of record in the minutes of the executive body of both the parent and the subsidiary. Two copies of both sets of minutes, identified by name, address, and date of submission, shall be obtained by the CSO processing the clearance of the subsidiary facility.

c. Parent firms at all levels of the inter-corporate structure shall be processed for FCL or formal exclusion. This shall include the ultimate parent as well as any intermediate subsidiaries through which it may exercise ownership and control of the cleared company. However, if the immediate parent of the subsidiary elects to be excluded, all other parents in the multi-level corporate group must also be excluded, unless an independent clearance need exists.

d. Activities of a contractor which are located in a given geographical area under the same CSO may qualify for a single FCL, if the following conditions hold true.

(1) The activities of the contractor are under the direct supervision or management responsible for the day-to-day operations of all activities.

(2) A centrally directed security program is maintained, covering all activities consisting of the following elements: same name, single mailing address 1/, single SPP applicable at all locations, a unified document control system so organized as to permit the prompt location of any classified document within the various activities by a review of the records maintained at one or more of the control stations established under paragraph 12, ISM, and all security matters are under single management control.

(3) The distance between the activities is such that the contractor is able to maintain daily supervision of their operations, including day-to-day surveillance of the security program. Normally, the distance between any of the activities should not exceed 1 hour ground traveling time, except where the extent of classified activity, such as that normal at a remote test site, is such that only a minimum of supervision is required.

1/ Although a single mailing address is required for record purposes, the CSO may authorize a facility to use other addresses for the purpose of receiving classified material from parties with whom a classified contractual relationship exists or from other facilities of the organization where the contractor is a MFO, provided such other addresses are either post office box addresses or locations that are physically a part of the contractor's cleared facility. The CSO should authorize the foregoing only where the use of single address will pose a significant administrative problem for the contractor.

(4) It is management's desire that FCL's be aligned to conform to the contractor's organizational structure. In all instances, the CSO shall solicit the opinion of management before reaching a decision as to the number of FCL's that will be granted.

(5) However, in the event management objects to the decision of the CSO, the entire matter, including all supporting documentation, shall be referred by the CSO, to the Director, DIS, ATTN: Deputy Director (Industrial Security), HQ DIS for resolution.

e. Small business pools approved either in accordance with Section 708 of the Defense Production Act of 1950, (reference (ee)) as amended, or in accordance with the Small Business Act, (reference (ff)), are eligible to negotiate or perform on classified contracts. If access to classified information is required for negotiation or performance on a contract, the pool itself, if awarded the contract, or the individual member acting for the pool, shall be processed for a FCL. In addition, other members of the pool shall be processed for FCL's as subcontractors if they will require access to classified information during negotiation or performance on a specific contract. A security procedure shall be developed in coordination between the contracting officer and the CSO's.

f. Temporary Help Supplier. A temporary help supplier is a subcontractor who dispatches personnel on his or her payroll to perform work on the premises of the using contractor or UA in accordance with the provisions of paragraphs 5ab, 41a, and 74, ISM.

(1) A temporary help supplier and its field, branch, or associate offices that have a valid parent subsidiary or multiple facility relationship are covered in paragraphs 72 and 73, ISM, respectively. The following paragraphs are concerned with:

(a) a temporary help supply grantor (hereinafter referred to as the grantor) who grants licenses to other individuals or firms to use the name, administrative support, method of operation or style of the grantor in a specific geographic area; and

(b) a licensee or franchise holder (hereinafter referred to as a licensee) that is owned and operated by a legal entity separate and distinct from the grantor, and is licensed or franchised to do business under the name, method of operation, or style of the grantor.

(2) Where the temporary help personnel are actually employees of, and on the payroll of the licensee, the licensee may be granted a FCL as provided for in the ISM.

(3) Where the temporary help personnel are employees of, and on the payroll of the grantor, normally there would be no valid basis for the licensee to be granted a FCL. As an alternative, a FCL may be granted in the name of the grantor at the address of the licensee if there is a valid requirement for employees of the grantor to have access to classified information at a contractor facility or UA activity, provided that:

(a) the grantor has a FCL at its HOF; and,

(b) an employee of the grantor, located on the premises of the licensee, is appointed as FSO for the grantor; or,

(c) an employer-employee relationship is established between the grantor and at least one or more employees of the licensee through execution of a separate written agreement between the parties or by insertion of a clause in the franchise or license agreement. The agreement or clause shall specifically provide that, for a consideration, one or more employees of the licensee will act as the FSO for the grantor in the territory covered by the license or franchise. One signed copy or certified true copy of the agreement or clause shall be furnished by the grantor to the CSO concerned.

(4) If the provisions of paragraphs (3)(a) and (b) or (3)(a) and (c) above are followed, a FCL may be granted to the grantor at the address of the licensee. This location will, for industrial security purposes, be considered as an operating facility of a MFO. Among other things, the SPP of the operating facility shall specify the functions and responsibilities of the FSO and the procedures for:

(a) processing PCL's including the granting of company CONFIDENTIAL clearances by the FSO;

(b) briefing and debriefing of the temporary help personnel in accordance with paragraph 5g, ISM -- although it is the responsibility of the temporary help supplier to have the "Security Briefing and Termination Statements (Industrial Personnel)" (DISCO Form 482) executed by the temporary help personnel, there is no objection if the using contractor also requires execution of the DISCO Form 482; and

(c) processing visit requests to the using contractors, which visits shall be considered as Category I visits as defined in paragraph 41a, ISM.

(5) In those rare cases wherein a licensee has license or franchise agreements with more than one grantor, a FCL may be issued in the name of each grantor. Similarly, if a contractor is engaged in a business which requires a FCL in connection with such business and, in addition, is a licensee for a temporary help supplier, a FCL may be issued in his or her own firm's name and another in the name of the grantor.

g. Commercial Carriers. A commercial carrier (see "Glossary of Terms," DoD 5220.22-C, reference (b)), is subject to Interstate Commerce Commission (ICC) and Civil Aeronautics Board (CAB) regulations or similar regulations of the state in which it operates. (In order to qualify for the shipment of SECRET material a commercial carrier must be approved by MTMC and granted a SECRET FCL by the CSO.)

h. Commercial Messenger Service. SECRET FCL's may be granted to contractors engaged in the intra-city (or local area) same-day delivery only of classified material between cleared contractors or between cleared contractors and a UA and/or the U.S. post office.

2-105 Consultants -- General Requirements.

a. PCL and/or FCL requirements for self-employed consultants to UA activities and contractors shall be determined in accordance with paragraph 2-106, 2-107, and 2-108.

b. In all cases, self-employed consultants shall have a valid PCL issued in accordance with the requirements of the ISM. Consultants are not eligible for access to classified information outside the U.S., the Panama Canal Zone, and U.S. trust territories and possessions, unless in official travel status of not more than 90 days in any 12-month period. Consulting firms and Type B Consultants shall be processed for a FCL in accordance with paragraph 2-102.

2-106 Consultants, Type A. The consultant does not possess classified material except at the using contractor's cleared facility, on the premises of the UA activity, or while on authorized visits. All requirements of the ISM apply to the consultant who, for security administration purposes only, shall be considered to be an employee of the UA. A Type A Consultant to a temporary help supplier is prohibited unless used solely by the temporary help supplier. *

a. The requirement for a separate FCL for the consultant (including the execution of the DD Form 441 and the DD Form 441s by the consultant), shall be waived, provided the using contractor or UA activity and the consultant jointly execute a certificate as follows.

(1) Except in connection with authorized visits: (i) classified material shall not be possessed by the consultant away from the activity of the using contractor or UA, (ii) the using contractor or UA shall not furnish classified material to the consultant at any other location than the premises of the using contractor or UA, (iii) performance of the consulting service by the consultant shall be accomplished at the activity of the using contractor or UA, and (iv) classification guidance will be provided by the using contractor or UA.

(2) The consultant shall not disclose classified information to unauthorized persons.

(3) The using contractor or UA shall brief the consultant as to the security controls and procedures applicable to the consultant's performance.

b. One copy of such certificate shall be furnished by the using contractor to his or her CSO. In the case of a consultant to a UA activity, the certificate shall be retained by the Commander or Head of that activity.

c. The consultant shall complete the forms required by paragraph 26, ISM. These forms shall be submitted to DISCO through the UA activity or the contractor for which the consulting service is to be performed. Each application for FCL shall be accompanied by a copy of the certificate prescribed in paragraphs a(1) and (2) above. The LOC (DISCO Form 560) shall be issued to the using contractor or UA activity, as appropriate.

d. Failure to accomplish the certification described above shall require the processing of a FCL as prescribed by paragraph 2-102, above.

2-107 Consultants, Type B. The consultant possesses classified material at his or her place of business or residence, and has full responsibility for security of the classified material in accordance with the provisions of the ISM.

a. A FCL is required for the consultant to cover the premises at which he or she will possess the classified material and perform the consulting services.

b. Consultants of this type shall be considered to be prime contractors to the UA activity or subcontractors to the using contractor.

c. The provisions of this regulation pertaining to contractors or subcontractors, as appropriate, shall apply.

2-108 Consultants, Type C. Consultants possess classified material at or their regular employers' cleared facilities, the consultants and their employers having agreed as to their respective responsibilities for security of the classified material. The clearance status and safeguarding ability of the consultants' regular employers shall be obtained from the employers' CSO prior to the disclosure or release of classified information to the consultants.

a. No requirement exists for separate FCL for such as consultant (including execution of the DD Form 441 and the DD Form 441s for the consultant), or to have an existing FCL raised, provided the employing facility and the employee who is acting as consultant to another contractor or to a UA activity are both cleared for access to at least the category of classified information as that to which the consultant will require access, and provided further that the employing facility and the employee who is acting as a consultant jointly execute a letter agreement to safeguard classified information for an employee performing consultant services (see appendix I, paragraph U, ISM) by which the employing facility and the employee who is acting as a consultant agree:

(1) to place classified material which the consultant-employee must have in his or her possession under the employing facility's accountability system;

(2) to incorporate procedures in the employing facility's SPP which prohibit the dissemination of the classified material within the facility, except that appropriately cleared personnel of the facility may be designated in writing on a strict need-to-know basis, to provide the consulting employee clerical, destruction, and reproduction services necessary to his or her performance as a consultant;

(3) to furnish the employee who is acting as a consultant a storage container so that the classified material shall be stored under his or her control -- access to the storage container shall be limited to the employee who is acting as a consultant and the minimum number of employees designated in accordance with paragraph (2) above, which are essential to support the consultant; and

(4) to advise the CSO immediately upon any change in the consultant's status as an employee of the facility.

b. One copy of the letter agreement shall be furnished by the employing facility to its CSO, and one copy to the contractor or UA employing the consultant's services.

c. In the event it is necessary to raise the consultant's PCL to a higher level (not above that of the employing facility), the consultant shall complete the forms required by paragraph 26, ISM, and submit them through the employing facility to DISCO with a copy of the letter agreement prescribed in paragraph a above. (If required to be cleared to a higher level than that of the employing facility, the consultant shall be processed for a separate FCL pursuant to paragraph 2-107 of this part and be required to maintain a security program fully independent of that of his or her employer.)

2-109 Consultants to User Agencies Employed Under Civil Service Procedures. Security clearances for persons employed as consultants to UA's under civil service procedures normally will be issued under the separate regulations of the UA concerned. However, UA's may process such a consultant for a PCL and/or FCL under the provisions of paragraphs 2-106, 2-107, or 2-108.

2-110 National Agency Check (NAC) (Facility).

a. A NAC of a facility shall include a check of the agencies indicated below:

- (1) Federal Bureau of Investigation (FBI);
- (2) Defense Central Index of Investigations (DCII),
Personnel Investigations Center, Baltimore, Maryland; and *
- (3) other agencies as appropriate.
- (4) For commercial carriers, a check shall also be made of the ICC for those carriers engaged in interstate surface transportation and the CAB for air carriers. State transportation regulatory bodies will be checked only when the carrier operates wholly within a state and is not part of interstate movement.

b. The CSO shall submit requests for NAC's to DISCO by letter and shall include the following identifying data concerning the facility:

- (1) full name, street address, city, and state of facility being cleared;
- (2) full name, street address, city, and state of the parent, in the case of a subsidiary;
- (3) any change in name or address of the facility being cleared which has occurred within the past 10 years; and
- (4) names and positions of OODEPs who are required to be cleared as a part of the FCL.

2-111 Requirements for Facility Security Clearances and Annual Review.
The actions to be accomplished by the CSO prior to granting a FCL to a contractor are prescribed in paragraph 2-116. Also, with respect to commercial carriers, see the procedures set forth in section I, of part 7.

a. For a FCL the following actions shall be accomplished.

(1) Conduct a DD Form 374 survey. For commercial carriers part I of the "Industrial Security Survey/Inspection (Commercial Carrier)," DIS Form 1148, (see paragraph 9-206.1) will be completed in lieu of the DD Form 374.

(2) Execute for the DoD the DD Form 441 or "Appendage to Department of Defense Security Agreement" (DD Form 441-1) and the DD Form 441s with the facility. For commercial carriers, the DIS Form 1149 and the DIS Form 1150 (see annexes B and C of reference (b)) will be executed in lieu of the DD Forms 441 and 441-1. The Directors of Industrial Security are designated as the authorized representative of the government for signing the DD Forms 441 and 441-1 and the DIS Forms 1149 and 1150.

(3) Request DISCO to obtain a NAC on the facility.

(4) Request DISCO to process PCL's, as appropriate, in accordance with paragraph 2-113. The DISCO shall furnish the CSO the undated LOC's. The CSO shall date and issue these LOC's concurrently with the "Letter of Notification of a Facility Security Clearance" (DIS FL-381-R) to the facility. For commercial carrier facilities, a "Letter of Notification of Facility Security Clearance for a Commercial Carrier" (see annex D, reference (b)) shall be issued to the facility.

b. For an interim FCL the following shall be done.

(1) Conduct a DD Form 374 survey. For commercial carriers part I of DIS Form 1148 will be completed in lieu of the DD Form 374.

(2) Execute the DD Form 441 or 441-1 and the DD Form 441s with the facility. For commercial carriers, the DIS Forms 1149 and 1150 will be executed in lieu of the DD Form 441 or 441-1. The Directors of Industrial Security are designated as the authorized representatives of the U.S. Government for signing the DD Forms 441 and 441-1 and the DIS Forms 1149 and 1150.

(3) For an interim TOP SECRET FCL, request DISCO to obtain a NAC on the facility. For interim SECRET and interim CONFIDENTIAL FCL's, request DISCO to ascertain from information available in the investigative files of the DCII whether adverse information exists concerning the facility.

(4) The CSO will request DISCO to process PCL's, as appropriate, for the level of clearance required for the personnel required to be cleared by paragraph 2-113. When appropriate, individuals shall be processed for interim PCL's. The DISCO shall furnish the CSO the undated LOC. The CSO shall date and issue these LOC's concurrently with the DIS FL 381-R.

c. A NAC of a facility of a MFU is not required where the HOF of such an organization has had a NAC conducted with favorable results.

(Inasmuch as a subsidiary of a parent-subsidary organization is a separate legal entity, this exception does not apply even though the parent has had a NAC conducted with favorable results.) Furthermore, a facility NAC (or check of the DCII in case of an interim SECRET or CONFIDENTIAL FCL) is not required when the name of the organization is the same as the name of one or more of the individuals who is being cleared in connection with the FCL. Similarly, a check is not required when the name under which the contractor is doing business has been adopted within the past 6 months. However, when there has been a recent change in the operating name of the business, a check should be requested on the former name or names under which the contractor or predecessor organization operated during the preceding 10 years, unless there has been a previous NAC conducted on the name.

d. FCL's shall not be granted by the CSO when any OODEP who is required to be cleared in connection with a FCL, as set forth in paragraph 2-113, is found to be ineligible for access to classified information under the standards and criteria established by the Industrial Personnel Security Clearance Program (see paragraph 2-121).

e. When a TOP SECRET FCL has been requested, the facility shall be granted a SECRET FCL as soon as the personnel who are required to be cleared pursuant to paragraph 2-113 are cleared at the SECRET level, provided of course, the facility is otherwise eligible for a SECRET FCL. (When a TOP SECRET PCL is requested for a U.S. citizen, DISCO automatically grants a SECRET PCL when the NAC is completed and supersedes this with a TOP SECRET PCL when the BI is completed.) Subsequently, when the required personnel are cleared for access to TOP SECRET material, a TOP SECRET PCL shall be granted.

f. A CSO may, at its discretion, elevate a requested CONFIDENTIAL FCL to the SECRET level if there is reason to believe that, because of the nature of the facility's business activity, there is a strong probability that the facility will have occasion to bid and/or perform on classified contracts at the SECRET level.

g. Prior to initiating any action to process a facility for a FCL, the CSO shall review the "Consolidated List of Debarred, Suspended, and Ineligible Contractors." Debarment and suspension actions, codes A and B, are considered pertinent from a security interest point of view. If so listed, the facility or OODEP would normally be ineligible for a security clearance. The CSO shall seek assistance from legal counsel before proceeding with further action.

h. FCL's shall not be granted by the CSO prior to the receipt of an adequate written SPP. An interim SPP is deemed to be adequate when it places into effect the requirements of the ISM which are immediately applicable to the operations of the facility in connection with the facility's anticipated involvement in the DoD Industrial Security Program.

i. Where a TOP SECRET FCL has been granted, the CSO shall review the facility on an annual basis to determine need for continuation of the clearance at the TOP SECRET level. Should there have been no possession of nor access elsewhere, and should there have been no bid, quote, or proposal submitted by the facility in response to a government procurement invitation during the preceding 3-year period which would have required contract performance at the

TOP SECRET level, the FCL shall be administratively downgraded to SECRET or CONFIDENTIAL, as appropriate. In the case of parent-subsidiary and MFO's, the prior coordination of the CSO's having an interest shall be obtained. In all cases, the following action shall be taken.

(1) Advise management of the facility in writing: (i) that the downgrading action does not reflect adversely upon the facility's security eligibility or ability to safeguard classified information, (ii) that the security clearances of all OODEPs and employees cleared at the TOP SECRET level will be downgraded without prejudice to the appropriate level, and (iii) that the FCL's facility and PCL's may be upgraded to the TOP SECRET level when a requirement for such exists.

(2) Prepare a new DIS Form 553 with the statement added under remarks: "TOP SECRET facility security clearance granted (date) is administratively downgraded in accordance with paragraph 2-111, DoD 5220.22-R." Submit to DISCO with a copy to DTIC, if appropriate.

(3) Forward a new DIS FL 381-R to the facility as notification of the new level of FCL.

(4) On receipt of the DIS Form 553, DISCO will issue new LOC's reflecting the appropriate level of access for the OODEPs and the affected employees, and will request the facility to return to DISCO the previous LOC's and any copies thereof.

2-112 RESTRICTED DATA, Additional Facility Security Clearance Requirements. Where access to RESTRICTED DATA as defined in the Atomic Energy Act of 1954 (reference (c)), as amended, is required by any prospective bidder or contractor, the additional security clearance requirement as prescribed in paragraph 2-312 shall have been satisfied prior to authorizing access.

2-113 Personnel Required to be Cleared for a Facility Security Clearance.

a. Corporations, Associations, and Nonprofit Organizations. Except as provided for below, the following individuals are required to be cleared in connection with (and at the level of) the FCL.

(1) The chairman of the board and all principal officers (see paragraph 1-251) must be cleared.

(a) Other officers ^{2/} who do not require access to classified information in the conduct of the organization's business and who do not occupy positions that would enable them to affect adversely the

^{2/} All officers, as defined by paragraph 1-251, are considered OODEPs of an organization, but not all OODEPs occupy positions required to be cleared in connection with a FCL.

organization's policies or practices in the performance of classified contracts, are not required to be cleared, provided the organization complies with the provisions of paragraph g below.

(b) Other officers who require access to classified information in the conduct of the organization's business, but at a level less than that of the FCL, may be cleared with a U.S. Government granted clearance at the lower level, provided they do not occupy positions that would enable them to adversely affect the organization's policies and practices in the performance of the higher level classified contracts, and the organization complies with the provisions of paragraph g below.

(2) All directors must be cleared unless one of the following options is elected.

(a) Directors who shall not require access to classified information in the conduct of the organization's business and who do not occupy positions that would enable them to affect adversely the organization's policies or practices in the performance of classified contracts are not required to be cleared, provided: at least a legal quorum of the board of directors or similar executive body shall be cleared, and, if the corporation or association conducts meetings with a pro tem chairman or by a rotating chairmanship, all board members who are eligible for or could sit as board chairman shall be cleared, and with respect to all uncleared directors, the organization complies with the provisions of paragraph g below.

(b) If the board has seen fit to delegate certain of its duties and responsibilities to a legally constituted executive committee, all members of this committee shall be cleared. Other directors are not required to be cleared, provided the committee has full executive authority to exercise management control and supervision for the corporation, including responsibility over all matters involving the security of classified information in the possession of the organization and provided further, with respect to all uncleared directors, the organization complies with the provisions of paragraph g below. Directors who are not members of this executive committee may be cleared, but only at the same level as the FCL and when this is done paragraph g below is not applicable in their case. Two copies of the board of directors' or similar executive body's resolution, excluding the board members from access to classified information and delegating this authority to the committee, shall be furnished to the CSO.

(3) Executive personnel must be cleared. The management official in charge at the facility and the FSO shall always be cleared in connection with the FCL.

(4) A current list of all OODEPs shall be maintained by the corporation and the CSO. The list shall designate by name those individuals granted a LOC, those who are being processed for a PCL, and those who have been excluded from access to classified information pursuant to the provisions of paragraph g below. Such lists shall be signed by an OODEP of the corporation.

b. Sole Proprietorships. The following individuals are required to be cleared in connection with (and at the level of) the FCL:

- (1) the owner;
- (2) all officers, if applicable; and
- (3) executive personnel (see paragraph 1-228). The management official in charge at the facility and the FSO shall always be cleared in connection with the FCL.
- (4) A current list of all OODEPs shall be maintained by the sole proprietorship and the CSO. The list shall designate by name those individuals granted a LOC, those who are being processed for a PCL, and those who have been excluded from access to classified information pursuant to the provisions of paragraph g below. Such lists shall be signed by an OODEP of the sole proprietorship.

c. Partnerships. Except as provided for below, the following individuals are required to be cleared in connection with (and at the level of) the FCL.

- (1) All general partners must be cleared.
- (2) All other partners must be cleared.
 - (a) Partners other than general partners, who do not require access to classified information in the conduct of the organization's business and do not occupy positions that would enable them to affect adversely the organization's policies or practices in the performance of classified contracts are not required to be cleared, provided the organization by official action of the general partners complies with the provisions of paragraph g below.
 - (b) Partners other than general partners who require access to classified information in the conduct of the organization's business, but at a level less than that of the FCL, may be cleared with a U.S. Government granted clearance at the lower level, provided they do not occupy positions that would enable them to adversely affect the organization's policies and practices in the performance of the higher level classified contracts, and the organization by official action of the general partners complies with the provisions of paragraph g below.

(3) If the partnership has seen fit to delegate certain of its duties and responsibilities to a legally constituted executive committee, all members of this committee shall be cleared in connection with the FCL. General partners who are not members of this executive committee may be cleared, but only at the same level as the FCL. Nonexecutive committee member general partners may be excluded, provided the committee has full executive authority to exercise management control and supervision for the organization, and with respect to these other partners, the organization complies with the provisions of paragraph g below. Two copies of the partnership's resolution delegating this authority to the committee shall be furnished to the CSO. The resolution shall specify those partners excluded

from access to classified information and those partners excluded from access to the higher level classified information, as appropriate.

(4) For executive personnel, the management official in charge of the facility and the PSO shall always be cleared in connection with the FCL.

(5) A current list of all OODEPs shall be maintained by the partnership and the CSO. The list shall designate by name those individual granted a LUC, those who are being processed for a PCL, and those who have been excluded from access to classified information pursuant to the provisions of paragraph g below. Such lists shall be signed by a partner or an executive of the partnership.

d. Colleges and Universities. Except as provided for below, the following individuals are required to be cleared in connection with (and at the level of) the FCL.

(1) The chief executive officer must be cleared.

(2) Those other officers or officials who are specifically and properly designated by action of the board of regents, board of trustees, board of directors, or similar type executive body must be cleared, in accordance with the institution's requirement as the managerial group having the authority and responsibility for the negotiation, execution, and administration of UA contracts. The institution shall furnish the CSO a copy of such designation of authority, from which the particular officers who are to be processed in connection with a FCL can be determined, and thereafter changes shall be furnished as they occur. If this requirement is not met, all officers shall be processed for a PCL in connection with the FCL.

(3) All regents, trustees, or directors must be cleared, unless one of the following options is elected.

(a) Regents, trustees, or directors who shall not require access to classified information in the conduct of the organization's business, and who do not occupy positions that would enable them to affect adversely the organization's policies or practices in the performance of classified contracts, are not required to be cleared, provided that at least a legal quorum of the board of regents, board of trustees, board of directors, or similar executive body shall be cleared and, if the college or university conducts meetings with a pro tem chairman or by a rotating chairmanship, all board members who are eligible for or could sit as board chairman shall be cleared; and with respect to all uncleared regents, trustees, or directors, the organization complies with the provisions of paragraph g below.

(b) If the board has seen fit to delegate certain of its duties and responsibilities to a legally constituted executive committee, all members of this committee shall be cleared. Other regents, trustees, or directors are not required to be cleared, provided the committee has full executive authority to exercise management control and supervision for the organization, including responsibility over all matters involving the security of classified information in the possession of the organization and provided

further, with respect to all uncleared regents, trustees, or directors, the organization complies with the provisions of paragraph g below. Regents, trustees, or directors who are not members of this executive committee may be cleared, but only at the same level as the FCL, and when this is done paragraph g below is not applicable in their case. Two copies of the board of director's or similar executive body's resolution delegating this authority to the committee shall be furnished to the CSO.

(c) If the board has seen fit to delegate certain of its duties and responsibilities pertaining to the protection of classified information to a managerial group of officers or officials of the college or university, and if because of this delegation the board will not be in a position to affect adversely the performance of classified contracts, the board may exclude itself from the requirement for its members to be processed for a PCL by complying with the provisions of paragraph g below. Election of this alternative will not preclude a regent, trustee, or director from being processed for a PCL if such clearance is necessary in connection with the individual's duties other than in the capacity of a regent, trustee, or director. However, in such cases the PCL shall be at the same level as the FCL. Two copies of the board of regents', board of trustees', board of directors', or similar executive body's resolutions excluding the board members from access to classified information and delegating this authority to the managerial group shall be furnished to the CSO.

(4) For executive personnel, the management official in charge of the facility and the FSO shall always be cleared in connection with the FCL.

(5) A list of all OODEPs shall be maintained by the college or university and the CSO. The list shall designate by name those individuals granted a LOC, those who are being processed for PCL's, and those who have been excluded from access to classified information pursuant to the provisions of paragraph g below. Such lists shall be signed by an OODEP of the college or university.

e. Commercial Carriers.

(1) The procedures set forth in paragraphs a, b, and c above are equally applicable to commercial carriers which are corporations, associations, sole proprietorships, or partnerships.

(2) The terminal manager and the FSO are required to be issued a PCL in connection with the FCL of a carrier terminal listed on the DIS Form 1150.

(3) Concurrent with, but not as a part of the FCL, a sufficient number of carrier custodians consistent with estimated operational necessity will be issued a PCL in the same manner as negotiators (see paragraph 2-115) to provide adequate protection of SECRET controlled shipments at each terminal listed on the DIS Form 1150. Additional carrier custodians will be processed for clearance after the FCL is granted based on operational requirements in the manner prescribed in paragraph 26, LSM.

f. Eligibility Determinations. Individuals who, as determined by the CSO, are not OODEPs yet exercise control over the management of the facility shall be processed for a determination of clearance eligibility to the

level of the FCL. Such individuals shall be processed, if, through stock ownership, proxy voting rights, majority ownership of securities, or some other method, they control the management of the facility and affect the appointment and tenure of officers, directors, or principal supervisory management personnel of the facility. A favorable determination of eligibility by DISCO will be entered into the PSCF. A LOC will not be issued to the contractor. If DISCO cannot make a favorable determination, DISCO will follow the procedures in paragraph 2-320. A FCL will not be issued until the matter is resolved.

g. Exclusion Procedures. This paragraph applies to those officers, directors, partners, regents, and trustees who, pursuant to the provisions set forth above, can be excluded altogether from the requirement for a PCL or who can be excluded from higher level access by virtue of possessing a PCL at a level below that of the FCL. In order to invoke these exclusion procedures, the organization by formal action of the board of directors, all general partners, or similar executive body shall affirm, as appropriate, the following.

(1) Such officers, directors, partners, regents, or trustees (designated by name) shall not require, shall not have, and can be effectively excluded from, access to all classified information in the possession of the organization and do not occupy positions that would enable them to affect adversely the organization's policies or practices in the performance of classified contracts or programs for the UA's. This action shall be made a matter of record in the organization's minutes of the board of directors, partnership, board of regents, or trustees, or similar executive body. Two copies of such minutes, dated and identified by the name and address of the facility, shall be furnished to the CSO.

(2) Such officers or partners (designated by name) shall not require, shall not have, can be effectively denied access to classified information at the higher level (specify higher level(s)), and do not occupy positions that would enable them to affect adversely the organization's policies or practices in the performance of the higher level (specify higher level(s)) classified contracts or programs for the UA's. This action shall be made a matter of record in the organization's minutes of the board of directors, partnership, board of regents, or trustees, or similar executive body. Two copies of such minutes, dated and identified by the name and address of the facility, shall be furnished to the CSO.

(3) In the event the organization does not comply with one or both of the above, as applicable, all officers, directors, partners, regents, or trustees shall be processed for a PCL at the level of the FCL.

h. Representative of a Foreign Interest. When a RFI (see paragraph 1-256) is required to be cleared in connection with a FCL, and the RFI has not been excluded in accordance with paragraph g above, the following procedures shall apply.

(1) When the statement required by paragraph 20k, ISM, has been executed, official notice of execution shall be made a matter of record in the organization's minutes by the board of directors or similar executive body. Two copies of the minutes shall be furnished the CSO.

(2) Failure to obtain a PCL for, or to exclude, a RFI shall make the facility ineligible for clearance, and any existing clearance shall be administratively terminated by the CSO. Such action is not appealable.

(3) In those cases where an individual, who is cleared in connection with the FCL, becomes a RFI, the contractor shall submit the report required by paragraph 6a(4), ISM, and in addition shall take the actions prescribed in this paragraph.

1. One copy of each resolution, statement, or certificate received by a CSO, in accordance with paragraphs a through g above, shall be forwarded to DISCO.

2-114 Foreign Nationals Serving as Officers, Partners, or Members of Boards of Directors. Corporations, associations, colleges, universities, partnerships, or other entities which have foreign nationals serving as partners, officers (other than principal officers of corporations and associations), or members of the board of directors may be issued a FCL by the CSO if they are otherwise eligible and are found not to be under FOCI, as set forth in paragraph 2-201, provided that the following conditions are met.

a. The partner, officer, or director who is a foreign national does not occupy a position that would enable him or her to affect adversely the facility's policies or practices in the performance of contracts for the UA's.

b. The partner, officer or director who is a foreign national can effectively be denied access to all classified information.

c. The exclusion from access to classified information of a partner, officer, or director shall be accomplished in the manner prescribed in paragraph 2-113g. Two copies of such minutes identified by name, address, and date of submission shall be obtained by the CSO.

d. In case the organization does not comply with this requirement, it shall be ineligible for a FCL.

e. The foregoing provisions of this paragraph do not apply to partners, officers, or directors who are citizens of countries with which the U.S. entered formal reciprocal arrangements, and who have been granted a reciprocal clearance in accordance with paragraph 2-323. In addition, the access limitations which apply under paragraphs 2-117a(1) through (7) of this part shall also apply to foreign nationals granted a reciprocal clearance even though employed by a U.S. firm which is not under a reciprocal FCL. A citizen of one of these countries who is chairman of the board of directors as well as a principal officer (that is, a position which pursuant to paragraph 2-113 requires that the individual be cleared as part of the FCL of a U.S. firm) shall be eligible for a reciprocal clearance (paragraph 2-323); however, the access limitations in paragraphs 2-117a(1) through (7) shall be applied to the facility. DIS Form 553 and FL 381-R, and DISCO Form 560 will all be annotated to reflect the access limitations of paragraphs 2-117a(1) through (7) and 31c(1)(a) through (g), ISM, as appropriate. UA's prior to any release of classified information to facilities cleared, in accordance with the above, will ascertain that the classified information to be released has been approved for release by an official who has been

delegated disclosure authority by the NDP-1 (reference (r)) and agency implementation.

2-115 Clearance of Negotiators. Negotiators designated by the contractor as being required to participate in the preparation of a bid or quotation may be processed for PCL's concurrently with, but not as a part of, the FCL. A FCL is not dependent upon the clearance of negotiators and changes in negotiators shall not affect the status of a FCL. PCL's for negotiators shall not be granted prior to the FCL. Subsequent to the granting of a FCL, negotiators are processed for PCL's in the normal manner prescribed by paragraph 26, ISM.

2-116 Procedures for Processing a Facility Security Clearance. Basic procedural steps necessary in processing a FCL are as set forth below 3/.

a. Justification for a Facility Security Clearance. Requests to process a contractor for a FCL are originated by a UA or by a cleared contractor or subcontractor thereof. Requests must be based on a bona fide procurement requirement for a contractor to have access to, or possession of, classified information in connection with: all aspects of precontract activity, including preparation of bids and proposals and precontract negotiations; the performance of a classified contract; all aspects of postcontract activity; and classified information not released or disclosed under a procurement contract, such as classified information released pursuant to a UA program participated in by a firm, organization, or individual on a voluntary or grant basis (for example, the long-range scientific and technical planning programs and programs designed to provide planning briefings for industry) 4/. It is U.S. Government policy to increase competition by publicizing procurements which offer competitive opportunities for prospective prime contractors or subcontractors 5/; thus assisting small business and labor surplus area contractors and broadening industry participation in DoD procurement programs. This policy is stated in the Federal Acquisition Regulation (reference (gg)), paragraph 5.001, and in the DAR (reference (c)), paragraph 5.001. Therefore, the requesting UA or cleared contractor, shall allow sufficient lead time in connection with the award of a classified prime or subcontract so the necessary FCL may be processed for a prospective contractor who does not currently possess a valid FCL. When the necessary processing cannot be accomplished within the time limits to qualify the prospective contractor for participation in the particular procurement action which gave rise to the

3/ In connection with the upgrading of a FCL the same steps, where appropriate, apply.

4/ Normally the facility will be processed for clearance at the classification level of the contract or program which gave rise to the request. However, where the underlying contract or program is at the CONFIDENTIAL level and the CSO determines that there is a reasonable likelihood the facility will require a SECRET FCL in the foreseeable future, the facility may be processed at the SECRET level.

5/ This includes contractors who will require visual and/or aural access in connection with work performed on a military installation.

request, the UA or prime contractor shall request the CSO to continue the clearance action in order to qualify the prospective contractor for future classified contract negotiations of a similar nature, provided:

(1) the delay in processing the FCL was not occasioned by a lack of cooperation on the part of the prospective contractor; and

(2) the UA or prime contractor is of the opinion that there is reasonable likelihood that the prospective contractor will participate in future classified contract negotiations and the contractor agrees to such participation.

b. Assumption of Security Cognizance. The CSO which has assumed cognizance shall forward a letter to the facility advising of such action and arrange a date for a security specialist to visit the facility. The CSO also shall submit an abbreviated (pending) "Central Index File Card-Facility" (DIS Form 553) to DISCO.

c. Initial Visit of Security Specialist. The initial visit to the facility shall be made within 10 calendar days after receipt of the request to process the contractor for a FCL. Exceptions may be granted for unusual cases at the discretion of the Regional Director, with the concurrence of the requester. However, action to initiate the clearance process, to include forwarding of applicable forms to the contractor, will be accomplished within 15 working days in these exceptional cases. When making the initial visit, the security specialist shall inform management concerning the DoD Industrial Security Program and furnish management the forms necessary for a FCL. The security specialist shall advise management of the facility of its responsibilities under the DD Form 441. This discussion shall include, but not necessarily be limited to:

- (1) the definition of a classified contract;
- (2) government responsibility for classification, and the contractor's source of guidance and clarification of classification instructions;
- (3) the role of the CSO;
- (4) the government's right of security inspections;
- (5) responsibility for security costs;
- (6) security responsibilities of the contractor if he or she awards or obtains a classified subcontract;
- (7) special security requirements that may be included in a contract;
- (8) the requirements, on completion of a contract, for destroying or returning all classified material provided or generated in connection with that contract;
- (9) the general policy concerning FOCI, and the requirement to execute the DD Form 441s;

(10) the requirement for the clearance of OODEPs in connection with the FCL — also provide guidance and advice to management in identifying the facility personnel who must be cleared in connection with the FCL;

(11) provisions for terminating the DD Form 441;;

(12) procedures for contractor-granted CONFIDENTIAL clearances;

(13) industrial security education;

(14) classified visit procedures;

(15) the importance of the SPP;

(16) the requirement for obtaining authorization for the establishment of any restricted or closed area;

(17) minimum storage requirements; and

(18) the general subject of PCL's. In this regard, explain that only personnel who have been granted a PCL are eligible for access to classified material and discuss the need-to-know principle. Point out the necessity for limiting the number of cleared personnel to only those required to perform tasks and services essential to the fulfillment of a contract or program. Instruct management on the preparation of personnel security forms and fingerprint cards and the procedures for submitting clearance requests. In the event an interim FCL has been requested, explain the need for the contractor to take immediate action to obtain clearances for those employees who will require access to classified information in order to perform on the contract which was the basis for requesting the interim clearance.

d. The security specialist shall conduct the DD Form 374 survey for the purpose of evaluating the ability of the facility to safeguard classified information of the same category as that of the FCL being processed and to determine the degree of FOCI, if any. Full completion of the DD Form 374 shall be accomplished as expeditiously as possible. In this connection the contractor shall be advised that any delay on his or her part in the execution and submission of the necessary forms, including the submission of PCL requests for those personnel who are required to be cleared in connection with the FCL, will delay the granting of the FCL.

e. Security Agreement and Related Forms.

(1) DD Form 441. The DD Form 441, "Department of Defense Security Agreement," is entered into between a contractor who will have access to classified information, and the DoD in order to preserve and maintain the security of the U.S. through the prevention of unauthorized disclosure of classified information. Requests for modifications to the security agreement shall be submitted through channels to the DUSD(P), ATTN: DSP&P. The security agreement once executed shall continue in effect until terminated by action of either party thereto in accordance with the "Article on Termination" contained in section IV of the agreement. The CSO shall execute the DD Form

441 on behalf of the DoD prior to granting a FCL, and an authorized official shall execute the agreement on behalf of the contractor.

(2) DD Form 441-1. At the option of management of a MFO, a DD Form 441-1, "Appendage to Department of Defense Security Agreement," may be incorporated in the DD Form 441, identifying by name and location each of the various facilities of the contractor to be covered by the agreement. Separate security agreements will not be necessary to cover the facilities enumerated in the appendage. On agreement between management and the CSO, additional facilities may be added or deleted from the original security agreement by using DD Form 441-1. When the HOF of a MFO submits a new DD Form 441, it is not necessary to obtain new DD Forms 441-1 for other facilities of the MFO. The existing DD Forms 441-1 may be attached to the new DD Form 441 by a letter indicating the date of change. The contractor is responsible for furnishing a copy of the security agreement, with appendage, to each individual facility listed thereon and to each concerned CSO. This paragraph shall not be construed to preclude the requirement for the accomplishment of all other FCL actions prescribed by this regulation.

(3) DD Form 441s. Simultaneously with the execution of the DD Form 441, management of the facility being processed for a FCL shall be required to execute the DD Form 441s, "Certificate Pertaining to Foreign Interests." The DD Form 441s executed by the HOF of a MFO will encompass all operating facilities of the organization. At least annually, inspectors should make an inquiry as to the accuracy and currency of the information reflected on the existing DD Form 441s, particularly if no changes had been reported to the CSO during the preceding year, in accordance with paragraph 6a(4)(f), ISM. The execution of this form shall be required for all companies being processed for a FCL 6/, and for uncleared parent organizations of cleared subsidiaries (see paragraph 2-104b). However, the CSO may require the accomplishment at an earlier time when some question pertaining to FOCI arises and the CSO believes that the execution of this form is in the best interest of the DoD.

i. Review of DD Form 441s. The factors to be used in determining the existence of FOCI are set forth in paragraph 2-202. If any of these factors are present in a facility being processed for a FCL, the CSO shall proceed in accordance with paragraph 2-203.

g. Documents to be Forwarded to DISCO. When the CSO has received all PCL applications necessary for a FCL, each form shall be conspicuously stamped OODEP. The PCL applications for the OODEPs and the request for the facility NAC shall be forwarded to DISCO. Submission of the facility NAC request shall not be delayed pending receipt of OODEP clearance applications. If one or more of the OODEPs is temporarily unavailable to complete the necessary forms, the submission of the clearance application for the other OODEPs and the request for the facility NAC shall not be delayed.

h. Follow-up Action.

6/ DD Form 441s is not required for each facility of a MFO.

(1) If the necessary clearance documents are not received within 15 calendar days after the initial visit, the CSO shall make an informal inquiry. If the forms are not received within 30 calendar days after the initial visit, a written inquiry shall be sent to the contractor advising that processing of the FCL will be discontinued unless the forms or an adequate explanation are received within 10 calendar days. A copy of the letter of inquiry shall be furnished to the activity which requested the FCL. If the necessary forms are not received from the contractor within 45 days after the initial visit and the contractor cannot justify a time extension, processing of the FCL shall be discontinued and the activity which requested the clearance action shall be so advised. The 15-, 30-, 45-day time span follow-up applies equally to those cases being processed as a result of changed conditions. (If a visit is not made, the time span commences from the date the facility is notified to furnish the necessary clearance documents.) When reprocessing a FCL and the contractor fails to submit the required forms within the time span indicated, the CSO shall notify the contractor in writing: (i) that the contractor's safeguarding ability will not be confirmed to any requesting contracting activity, and (ii) that his or her failure to submit the forms requested by the CSO is a violation of paragraphs 21a and 26a, ISM, as applicable.

(2) If the facility being processed is a subsidiary or a facility of a MFO, the FCL of the parent or the HOF shall be checked by the CSO to ensure that the FCL of the parent or HOF is valid and of the appropriate classification level. This check shall be made with the CSO of the parent or HOF.

(3) The CSO shall follow up with DISCO if OODEP clearances or results of a facility NAC are not received within a reasonable period of time.

1. Final Actions. The CSO shall ensure that all forms have been properly completed, facility NAC has been satisfactorily completed, and that clearances have been received from DISCO for those persons required to be cleared in connection with the FCL or that exclusion statements are held. The CSO shall execute and distribute those forms not previously distributed to the facility. The requesting UA or prime contractor shall be advised that the FCL has been granted.

j. DoD Technical Information Dissemination Activities.

(1) "Facility Clearance Register" (DD Form 1541) shall be used for the certification of FCL and safeguarding ability. When a contractor has an initial requirement to receive classified material from the DTIC; its field extensions; a DoD Information Analysis Center; or the Redstone Scientific Information Center, U.S. Army Missile Command, Redstone Arsenal, Alabama; the contractor shall submit a DD Form 1541 directly to the CSO. Resubmission of the DD Form 1541 by the contractor to meet subsequent requirements for services on other contracts is not required. The CSO will complete part II of the DD Form 1541 and forward the form to: DTIC, Cameron Station, Alexandria, Virginia 22314. Thereafter DTIC shall advise its field extensions, the DoD Information Analysis Centers, and the Redstone Scientific Information Center of the clearance and safeguarding ability of using contractors as required. The CSO shall indicate in the facility file that the FCL and safeguarding ability have been certified to DTIC. If there are any subsequently changed

conditions affecting the FCL or safeguarding ability, the DTIC shall be notified immediately. Such notification will be submitted by a copy of the DIS Form 553. Whenever the nature of the changed condition may not be readily apparent to DTIC from the copy of the DIS Form 553, the CSO shall include an appropriate notation under "Remarks" on the DIS Form 553, stating precisely the condition that affects the contractor's eligibility for the service. Such notifications shall always be included when the facility's safeguarding ability has changed. Once a DD Form 1541 has been certified by the CSO, it shall remain in force for all subsequent requests for "Registration for Scientific and Technical Information Services" (DD Form 1540) and need not be recertified except where there has been a change in facility conditions which require recertification by the CSO.

(2) The DD Form 1540 is used to certify the contractor's need-to-know for information distributed by DoD technical information documentation activities. In addition to the DD Form 1541, the contractor's need-to-know information within specified DoD interests must be determined in order to establish the contractor's eligibility for classified services. This need-to-know decision is made by the PCO (pursuant to DoD Instruction 5200.21, reference (hh), and the UA implementing instructions) on the basis that information in a particular field of interest is needed by the contractor in connection with work being performed under the contract. Separate DD Forms 1540 are required for each contract under which the contractor desires to receive secondary distribution of scientific and technical information services within particular fields of interest. The DD Form 1540 is then submitted directly to the contracting officer for approval. In the case of a prime contract, the DD Form 1540 must be approved by the PCO. In the case of the subcontract the DD Form 1540 may be approved by the ACO, provided the ACO verifies that the particular field of interest is required in the performance of the subcontract and is within the scope of the field of interest previously approved by the PCO on the prime contract. The PCO will provide a copy of the approved DD Form 1540 to the ACO when required. If no field of interest has been established on the prime contract, the subcontractor's request must be certified by the PCO. Approved DD Forms 1540 are sent to DTIC. When DTIC receives the DD Form 1540, it will determine that there is a DD Form 1541 on file and thereafter establish the contractor's eligibility to receive scientific and technical information. Eligibility established on a DD Form 1540 remains in effect for the expected duration of the contract as established by the projected completion date supplied on the DD Form 1540, except where DTIC is notified by the ACO that the contract has been terminated or that the contractor's eligibility has been canceled based on advice from the CSO that the contractor is no longer capable of adequately safeguarding classified information. Prime and subcontractors may not retain such classified material following the completion or termination of the classified contract, except when authorized in accordance with paragraph 7-106.

(3) Facilities granted a Reciprocal facility security clearance by the cognizant security office are to be processed for eligibility for access to DoD classified technical information in the same manner as outlined in (1) and (2) above. Once eligibility has been established at DTIC, and subsequent document requests are properly received, DTIC shall release the requested documentation directly to the contracting officer who certified the contractor's need-to-know on the applicable DD Form 1540.

*
*
*
*
*
*
*

Under no circumstances will classified material be transmitted directly to reciprocal cleared facilities by the DTIC. It is the responsibility of the contracting officer to effect appropriate coordination to ensure that pertinent documents do not contain prescribed information (see paragraph 2-117a) and that they have been approved for release under the National Disclosure Policy prior to forwarding the material or otherwise providing the Reciprocal cleared facility access to the information requested. *

2-117 Facility Security Assurances.

a. The DoD has entered into bilateral reciprocal industrial security agreements with certain foreign governments. Under these bilateral agreements, a firm in one signatory country which is under the ownership, control, or influence in the other signatory country may be given a security assurance in accordance with the procedures established in these agreements. As an exception, contracts which involve the following types of classified information shall not be awarded to a U.S. firm cleared under these agreements for access to U.S. classified information:

- (1) RESTRICTED DATA as defined in the U.S. Atomic Energy Act of 1954, reference (o), as amended;
- (2) FORMERLY RESTRICTED DATA removed from the RESTRICTED DATA category pursuant to Section 142(d) of reference (o), as amended;
- (3) Canadian "Classified Atomic Energy Data" as defined in the Atomic Energy Control Act (revised Statutes of Canada, 1952) and the Atomic Energy Control Regulations, Order-in-Council PC, 1959-1643; *
- (4) COMSEC information (see paragraph 7-102g);
- (5) any ACDA classified information;
- (6) information for which foreign dissemination has been prohibited in whole or in part;
- (7) information for which a special access authorization is required; and,
- (8) any information which has not been specifically authorized for release to the government of the signatory country involved.

b. The DIS, or the designated agency of the signatory foreign government entering into the reciprocal industrial security agreement with the DoD, when requested to furnish a security assurance for a firm to the other government, will assume responsibility for processing the clearance action. The standards and requirements governing the granting of security clearances for the protection of its own classified information will be followed. If the firm does not have a FCL or has a FCL for a classification category lower than that which is requested, action shall be taken to grant a FCL or to raise a FCL to the required level.

c. The DIS shall accept a security assurance regarding a firm located in a signatory country under a reciprocal industrial security agreement which it requested from the designated foreign government agency. Likewise, the designated foreign government agency shall accept a security assurance which it requested from DIS. However, any clearance of a firm based on a security assurance which has been given under the procedures in this paragraph is subject to review by the government which granted the FCL in the event that derogatory information is developed following clearance action. Such a review will also be made when requested by the government which asked for the security assurance. The requesting U.S. activity, or designated foreign government agency, will be notified promptly of suspension of the FCL or of action to revoke or terminate it.

d. Except as otherwise stated in this paragraph, the requirements of this regulation shall be followed by the CSO in granting a FCL or raising one to the level required. If the CSO develops credible information at any time during the clearance process which indicates that the firm is not eligible for or should be denied clearance, the pertinent facts will be

reported promptly to DISCO. Similarly, if DISCO develops serious derogatory information in connection with processing the PCL on any of the individuals required to be cleared in connection with the FCL pursuant to paragraph 2-113, appropriate documentation will be prepared. In either event, DISCO will request the Director for Industrial Security Clearance Review (DISCR), Office of the General Counsel (OGC), OSD (a copy of the complete correspondence will be forwarded to the HQ DIS) to determine whether the clearance action should be continued and what notification, if any, should be given the designated foreign government agency requesting the assurance, and whether action to deny a FCL shall be processed under the provisions of paragraph 2-121.

e. When favorable clearance action has been completed, the CSO shall record the clearance in the PSCF by submitting the original completed DIS Form 553. A copy of the DIS Form 553 will be forwarded direct to DISCO for use in giving a security assurance. A modified DIS FL 381-R shall be used by the CSO to notify the facility of such clearance and its purpose.

2-118 Changed Conditions Pertaining to the Facility. When changed conditions occur in the facility, the first consideration shall be the safeguarding of classified information to which the facility has current or impending access. Action to ensure the safeguarding of the classified information shall be taken immediately upon an initial determination that conditions have changed. FCL's should not be immediately invalidated because of changed conditions described in paragraph a, b, or c below, when: (i) the facility is currently performing on classified contracts, is in possession of classified information, or both; (ii) the CSO determines that classified information in possession of the facility can be safeguarded adequately and, in the case of a change of ownership or management, that the new owners, officers, and so on, can and will be effectively denied access to classified information pending completion of their PCL actions; and (iii) the required PCL or FCL forms are promptly submitted for processing. (Unless the new personnel are expected to be cleared within 15 days, an exclusion certificate, similar to that required by paragraph 2-113g, signed by a cleared owner, partner, officer, or executive personnel in charge of a facility, shall be obtained as assurance of the contractor's intent to deny access to uncleared owners, officers, and the like.) Observance of these guidelines will lessen administrative workload of the CSO and reduce to a minimum the occasion when it is necessary to invalidate a FCL. In all instances where the changed condition affects the clearance or safeguarding capability of a facility that has been certified to DTIC for classified services, a copy of the DIS Form 553 which is submitted to DISCO shall also be sent to DTIC.

a. Change of Operating Name.

(1) In the instances of changes in the operating name of the facility when ownership and management remain the same, the FCL shall be processed promptly to a valid status if the facility has a current procurement requirement for access to classified information or has classified information in its possession.

(2) If the facility does not have current access to classified information, and does not have possession of classified information, the clearance need not be processed to a valid status. However, a DIS Form 553,

appropriately annotated to reflect the defective FCL and the reason for it, shall be placed in the files of the CSO and DISCO. If appropriate, action shall be initiated under paragraph 2-119 for administrative termination of the FCL.

(3) If the FCL is to be processed to a valid status the following actions shall be completed.

(a) A new DD Form 441 shall be executed.

(b) A DIS FL 381-R shall be issued.

(c) A DIS Form 553 shall be submitted under the new operating name to DISCO, indicating in item 11 the specific reasons for such submission and noting the administrative termination of the FCL under the old operating name. The CSO shall forward a pending DIS Form 553 reflecting the new name of the facility immediately following receipt of a report of a name change. Include in block 11 of the form a cross reference to the existing DIS Form 553 (including prior editions of this form) in PSCF and the specific reason for submission. This will permit DISCO to accept and process PCL's for the facility pending receipt of the DIS Form 553 to be submitted when all actions to process the FCL to a valid status have been completed. Of course, if it is possible to do so, a complete DIS Form 553 should be sent at once to DISCO instead of a pending DIS Form 553. In addition, DTIC shall be notified as required by paragraph 2-116j.

b. Changes in Ownership or Management.

(1) In instances of changes of OODEPs, the FCL must be processed promptly to a valid status, provided the facility has a current procurement requirement for access to classified information or has classified information in its possession. Classified information shall not be furnished to nor shall retention by the facility be permitted unless the CSO can assure itself that classified information can be safeguarded and that the new owners or management shall not obtain access to the classified information while their clearances are being processed. The CSO shall make this assurance on the basis of a visit to, or communication with, the facility and a discussion with the new owner or management and the FSO as to the procedures that will be put into effect. When the change in management occurs because a cleared employee is elevated to the position of an OODEP, the CSO shall advise DISCO and DISCO will amend the DISCO Form 560 for the individual to reflect the change.

(2) If the facility does not have a procurement requirement for access to classified information and does not have any classified information in its possession, the FCL shall be invalidated. A DIS Form 553, appropriately annotated to reflect the invalidation and the reasons for it, shall be placed in the files of the CSO with the original forwarded to the DISCO. If appropriate, action shall be initiated under paragraph 2-119 for administrative termination of the FCL.

(3) If the FCL is to be processed to a valid status, the following actions shall be completed.

(a) Clearance action for the new personnel shall be started promptly for clearance to the level of the FCL. (A certificate specifically excluding such personnel by name and title from access to classified information until such time as they are appropriately cleared shall be obtained from the contractor for retention in the files of the CSO.)

(b) In the case of a sole proprietorship or a partnership, a new DD Form 441 shall be executed and a new DIS FL 381-R shall be issued.

(c) In all cases involving a change of ownership, a new DD Form 374 survey shall be completed, to include execution of a new DD Form 441s. The new owner or management will be advised of the need to promptly forward the required PCL and FCL forms to the CSO. The CSO shall determine whether a new certificate is required in connection with changes in officers, directors, partners, regents, trustees, or executive personnel.

(d) On completion of the above actions, a new DIS Form 553 shall be submitted, indicating in item 11 the specific reasons for such submission.

c. Change of Address.

(1) In instances in which a facility is relocated, if the facility has current procurement requirement for access to classified information or has classified information in its possession, the FCL shall be processed to a valid status.

(a) A complete DD Form 696 inspection shall be conducted immediately to assess continuing applicability of facility security procedures and safeguarding of classified information.

(b) A supplemental DD Form 374 survey shall be completed to amend those portions of the previous survey pertaining to the relocation.

(c) The existing DD Form 441 (or the DD Form 441-1 when appropriate) shall be amended to reflect the change in address of the facility or, where administratively more feasible, a new DD Form 441 or 441-1 shall be executed.

(d) A DIS FL 381-R shall be issued.

(e) A DIS Form 553 shall be submitted for the facility at the new address indicating in item 11 reasons for such submission and noting the administrative termination of the FCL at the old address. The CSO shall forward a pending DIS Form 553 reflecting the new address of the facility immediately following receipt of report of an address change. Include in item 11 of the form a cross reference to the existing DIS Form 553 in the PSCF and the specific reason for submission. This will permit DISCO to accept and process PCL's for the facility pending receipt of the DIS Form 553 to be submitted when all actions to process the FCL to a valid status have been completed. In addition, DTIC shall be notified as required by paragraph 2-116j. Of course, if it is possible to do so, a complete DIS Form 553 shall be sent at once to DISCO instead of a pending DIS Form 553.

(2) If the change involves only a change of address, with no relocation of any elements of the facility, the actions indicated in paragraphs (1)(c), (d), and (e) above shall be completed.

(3) If the facility does not have a current procurement requirement, does not possess classified information, and it is otherwise appropriate, action shall be initiated under paragraph 2-119 for administrative termination of the FCL.

d. Closing of Business and Bankruptcy. In all instances in which information is received by the CSO that a facility previously granted a FCL has closed its doors, gone out of business, been adjudicated, bankrupt, and so on, the CSO shall administratively terminate the FCL (see paragraph 2-119). This shall include the withdrawal of DIS FL 381-R and termination of the DD Form 441. This information shall be processed promptly to DISCO using DIS Form 553 and stating the reasons for such submission under item 11. In addition, a copy of the new DIS Form 553 shall be sent directly to DTIC. All classified information shall be recovered promptly from the facility by the CSO in coordination with contracting UA(s). A "close-out" inspection shall be conducted to assure that proper action has been taken. All actions taken to ensure proper disposition of classified material shall be indicated under "Remarks" on the DD Form 696.

e. Personnel Actions Affecting a Facility Security Clearance. Whenever a PCL for an individual who is required to be cleared in connection with a FCL pursuant to paragraph 2-113 is denied, revoked, suspended, or withdrawn the provisions of paragraph 2-121d apply.

f. Changes Involving Representatives of a Foreign Interest. Where citizens or immigrant aliens are required to be cleared in connection with the FCL and these individuals fall within the definition of RFI, the procedures set forth in paragraph 2-113h shall be followed. In the event personnel previously cleared in connection with the FCL become RFI's, the contractor is required to report this change to CSO and the procedures set forth in paragraph 2-113h shall be followed.

g. Placement of Contractor on Debarred Bidders' List. Each issue of the "Consolidated List of Debarred, Suspended, and Ineligible Contractors" shall be reviewed to determine whether any facilities under security cognizance have been listed. Instructions are located in the front of each issue of the list. Debarment and suspension actions, codes A and B, are considered pertinent from a security interest point of view. If a facility is so listed, the CSO shall seek assistance from legal counsel before proceeding with further action. If warranted by the circumstances, the CSO shall do the following.

(1) Invalidate the FCL. The FCL and safeguarding ability shall not be verified.

(2) A DIS Form 553, annotated to reflect the invalidation and the reasons for it, shall be placed in the files of the CSO, DISCO, and DTIC, if appropriate.

(3) If the facility has current access to classified information, UA's of record shall be notified of the invalidation. On receipt of this notification, the UA contracting officer will determine whether the facility may continue to perform on existing classified contracts and notify the facility and the CSO as soon as possible. If the response indicates that continued processing of PCL's is necessary, DISCO shall be so advised.

(4) The facility shall be notified that the FCL is invalid, that performance on existing contracts may be continued pending final determination by the UA contracting officer, and that access to additional information or contracts will not be permitted until the debarment or suspension is terminated.

(5) Administratively terminate the FCL if the contractor is not performing on a classified contract and is no longer in possession of, or having access to, classified information.

h. Changes Involving a Parent Organization. Whenever the FCL of a parent organization is terminated, the CSO of all subsidiaries of the parent that have a FCL shall be immediately notified. In this event, the FCL of the subsidiaries shall also be terminated, unless the exclusion procedures set forth in paragraph 2-104b can be applied. Similarly, if the clearance of the HOF of a MFO is terminated, the clearance of all operating facilities will also have to be terminated.

i. Upgrading of a Facility Security Clearance. Where a FCL is to be upgraded, the following actions shall be taken.

(1) A DIS Form 553 shall be submitted to DISCO, indicating in item 11 the specific reason for such submission.

(2) The facility shall be granted a new LOC reflecting the current level of the FCL.

j. Distribution List Notifications. The PIC-CVA, or the CSO if * appropriate, shall, when it has previously verified the FCL and safeguarding * capability of a facility in accordance with paragraph 1-110e, or paragraph 5x, ISM, and continuing distributions of classified material under the terms of the contract or program is specified, immediately notify the releasing contractor and the UA contracting activity when information is received which would adversely affect the FCL and safeguarding capability within one year of the * initial verification, or reverification. *

k. Changes Involving FOCI.

(1) In all instances of changes involving FOCI, actions required by paragraph 2-203 shall be promptly taken.

(2) When the elements of FOCI are extensive (see paragraph 2-203c), the FCL shall be invalidated by the CSO and the FCL and safeguarding capability shall not be verified.

(a) A DIS Form 553 annotated to reflect the invalidation and the reasons therefore shall be placed in the files of the CSO, DISCO, and DTIC, if appropriate.

(b) If the facility has current access to classified information, UA's of record shall be notified of the invalidation and the actions initiated to nullify the FOCI elements. On receipt of this notification, the UA contracting officer will determine whether the facility may continue to perform on existing classified contracts and notify the facility and the CSO as soon as possible. If the response indicates that continued processing of PCL's is necessary, DISCO shall be so advised.

(c) The facility shall be notified that the FCL is invalid, that performance on existing classified contracts may be continued pending final determination by the UA contracting officer, and that access to additional classified information or contracts will not be permitted until all FOCI elements are resolved.

(d) If after 30 days the facility fails to submit an acceptable plan for prompt and effective resolution of the FOCI elements, or if the facility subsequently fails to adhere to such plan, the matter shall be referred to the Director, DIS, ATTN: Deputy Director (Industrial Security), in accordance with paragraph 2-203c for consideration of revocation of the FCL.

2-119 Administrative Termination of a Facility Security Clearance.

a. An annual review shall be made by the CSO of facilities under its cognizance for the purpose of determining those facilities for which a FCL is no longer required. Generally, a FCL shall be administratively terminated when the contractor has not had an active classified contract or project for the preceding 9 months, has not been afforded authorized access during the preceding 9 months, and has no immediate prospects for obtaining a classified contract. When a facility has not had a classified contract or project for the preceding 9 months, but has classified material in its custody, the UA which approved the retention shall be requested to determine if there is a continuing requirement for the facility to retain custody of the classified material. Where there is not a continuing requirement for the facility to retain classified material, the actions set forth in paragraph b below shall be taken. *

b. When, on the basis of the foregoing guidance, the CSO determines that a FCL should be administratively terminated, or the contractor requests termination of the FCL in accordance with section IV, DD Form 441, a "close-out" inspection shall be conducted and the following action shall be taken at its conclusion.

(1) Advise management of the facility in writing as follows.

(a) The existing FCL's and PCL's will be administratively terminated unless management can satisfactorily justify within 30 days the need for the retention of their FCL.

(b) The proposed action in no way reflects adversely upon the facility's security eligibility or ability to safeguard classified information.

(c) The facility may be processed for a new clearance with a minimum of delay when the occasion and need arises for the facility to perform on classified work or otherwise require access to classified information.

(2) On completion of above action and 30 days after the notification to management, if management does not justify the need for the retention of the FCL, the CSO shall administratively terminate it. This requires the administrative withdrawal of the DIS FL 381-R and termination of the DD Form 441. The DIS Form 553 shall be forwarded promptly to DISCO stating the reasons for termination. In addition, a copy of the new DIS Form 553 shall be sent directly to DTIC, if the facility had previously been certified as eligible for DTIC classified services. The DISCO will administratively terminate all PCL's previously issued to the facility, and where an investigation is in process, arrange for its cancellation. However, "Personnel Security Clearance Change Notification" (DISCO Form 562) will be held for 25 months in the PSCF.

(3) If at the time of the "close-out" inspection (see paragraph 4-300) conducted just prior to the administrative termination of the FCL, the facility was not in possession of classified information, this fact should be indicated under "Remarks" on the DD Form 696. Should the facility be in possession of classified information, it shall be recovered from the facility by the CSO in coordination with the UA prior to termination of the FCL. All actions taken to assure proper disposition of classified material shall be indicated under "Remarks" on the DD Form 696, "Industrial Security Inspection Report," in accordance with paragraph 4-300.

c. Examples of justification for retention of a FCL are: an impending request for a bid or quotation on a classified contract from a UA or a prime contractor; planned attendance at a forthcoming classified meeting of the type described in paragraph 5q, ISM, which is supported by a contracting officer; current preparation of an unsolicited proposal containing classified information; or receipt by the CSO of a written request from a UA requesting that the facility retain its FCL because of the imminent award of a classified contract, because of a continuing requirement for use of the facility as a bid source, or because of the facility's unique capabilities. Justification for retention of a dormant FCL shall be revalidated annually in writing by the UA or contractor requiring the retention of the FCL.

2-120 Reprocessing or Revalidating a Facility Security Clearance.

a. In the event a classified procurement need arises after the FCL has been terminated, the CSO shall reassume cognizance and process a new FCL in accordance with this regulation. If processing occurs within 12 months after the termination, PCL's valid at the time of termination may be revalidated by notifying DISCO. This is accomplished by DISCO Form 562 in the same manner

as a reemployment. In the case of an OODEP, the DISCO Form 562 is submitted to DISCO by the CSO with an appropriate letter of explanation.

b. Before a facility with a defective FCL can be granted access to classified information in connection with a new contract, action shall be initiated to process the clearance to a valid status. In processing a defective FCL to a valid status, the following specific actions shall be taken by the CSO.

(1) The "Central Index File Request" (DD Form 555) shall be used to secure copies of the existing records from DISCO in all instances where the files of the CSO are not complete.

(2) The name and address of the facility shall be verified or corrected.

(3) The names and positions of the facility OODEPs cleared in connection with the original FCL shall be verified as still occupying the position and being appropriately cleared. If different persons appear in any of these positions, they shall be appropriately cleared, or their PCL's verified.

(4) If appropriate, a DD Form 441 and/or a DD Form 441s, shall be executed.

(5) A DD Form 374 shall be conducted.

(6) A new DIS Form 553 based on the verified or corrected information shall be completed and forwarded to DISCO.

(7) A new DIS FL 381-R based on the verified or corrected information shall be forwarded to the facility. This new DIS FL-381-R shall supersede and replace all others held by the facility.

2-121 Denial, Suspension, or Revocation of a Facility Security Clearance.

a. A FCL shall not be granted by the CSO unless the requirements of paragraph 2-111 have been satisfactorily completed.

b. When any OODEP (unless excluded as prescribed in paragraph 2-113g) required to be cleared in connection with the FCL is considered to be unsuited for access to classified information under the standards and criteria promulgated in the Industrial Personnel Security Clearance Program, DISCO shall submit a recommendation for the denial, suspension, or revocation of his or her PCL together with a copy of the report of investigation to the DISCR, OGC, OSD. The letter shall advise that the denial, suspension, or revocation will affect the FCL and accordingly priority handling shall be requested. In the event interim action is warranted in the interests of national security, DISCO shall take action in accordance with paragraph 2-320c.

c. In the event that a determination is made under the Industrial Personnel Security Clearance Program that the individual concerned is eligible to be cleared, the DISCR shall notify DISCO who, in turn, shall advise the CSO which shall grant or revalidate the FCL, as appropriate.

d. In those cases in which individuals, required to be cleared as part of a FCL under the provisions of paragraph 2-113 are denied PCL's or have their PCL's suspended or revoked by action of DISCR, DISCR shall notify the Director, DIS, ATTN: Deputy Director (Industrial Security), who shall, in turn, notify the CSO of the facility involved and DISCO. On receipt of this notification, DISCO shall immediately record the DISCR decision pertaining to the individual in the PSCF. The CSO shall immediately notify the facility that its FCL will not be granted or that it will be suspended or revoked unless one of the following conditions is met.

(1) In the case of individuals who have had their PCL's suspended, the facility furnishes positive assurance that such individuals will not have, and can be effectively excluded from, access to all classified information in the possession of the facility and that the individuals will not be in a position that would enable them to affect adversely the organization's policies or practices in the performance of classified contracts pending a final DISCR decision on the suspension action.

(2) In the case of individuals who have had their PCL's denied or revoked, the facility takes immediate action to remove the individuals concerned from their official positions and furthermore, furnishes positive assurance that they will not have, and can be effectively excluded from, access to all classified information in the possession of the facility.

(3) In each instance in which a company seeks to give such assurances, the following guidelines shall be taken into account:

(a) the position which the company officials hold and the extent of their ownership of the company, if any — for example, it would be very difficult to accept the company's assurance that a president of a company or an OODEP owning or controlling a sizable amount of stock could be denied access to classified information or control over the administration of classified contracts;

(b) the seriousness of allegations which led to the suspension of the company officials' PCL's — charges of subversive activity raise very grave questions with respect to the desirability of permitting the retention of high ranking company officials in their office pending the outcome of their security cases; and *

(c) the actions which the facility has taken to relieve the officials of their authority and the degree to which they have been removed from access to classified information. For example, a company might place officials whose clearances have been suspended on official leave or, if they continue on in active status, transfer them to a facility having no classified contracts. In such a case, provided notice that these officials' clearances have been suspended is given to the other company officials, it may be appropriate to withhold action that would revoke the FCL.

(4) In summary, this paragraph must be considered in the light of all facts of a particular case. The fact that officials have been removed from their offices or given different titles, pending determinations of their security cases, does not of itself provide the positive assurance that they can be effectively denied access to classified information. The officials'

inherent power and authority, and with it the likelihood of access to classified information, requires close scrutiny. Whenever there is any doubt as to the sufficiency of the action taken by the contractor pursuant to paragraphs (1) or (2) above, the CSO shall immediately request advice from the Director, DIS, ATTN: Deputy Director (Industrial Security).

(5) In all cases where DISCR has denied, revoked, or suspended the FCL of an OODEP, the CSO shall complete the actions prescribed by this paragraph and paragraph e below, pertaining to the affected facility, within 5 working days of notification of the DISCR decision. If the action is not accomplished with the prescribed time, the CSO shall formally advise the Director, DIS, ATTN: Deputy Director (Industrial Security), through the Regional Director, of the reason for the delay.

e. If the facility does not take prompt positive action as required in paragraph d above, the CSO shall be responsible for the following.

(1) If the contractor is not performing on a current classified contract, suspend or revoke the FCL, as appropriate. In this connection the CSO shall take immediate action to recover all classified information in the contractor's possession.

(2) If the contractor is performing on a classified contract, the CSO shall take immediate action to ensure that all classified information in the contractor's possession is being effectively safeguarded. The CSO shall coordinate with the contracting officer of the UA concerned who shall determine whether to terminate or continue the contract. If the UA's decision is to continue the contract, the CSO shall notify Director, DIS, ATTN: Deputy Director (Industrial Security) and supply a full statement of the facts. The CSO shall take appropriate action to ensure that the contractor is permitted access only to that classified information necessary in the performance of the contract concerned. All other classified information in the contractor's possession shall be recovered. If the UA's decision is to terminate the contract, the CSO shall suspend or revoke the FCL, as appropriate, and take immediate action to recover all classified information in the contractor's possession. The action taken shall be reported promptly to DISCO through the submission of a DIS Form 553, with a copy of the DIS Form 553 sent to the DUSD(P), ATTN: DSP&P, The Pentagon, Washington, D.C. 20301 and Director, DIS, ATTN: Deputy Director (Industrial Security). The DTIC shall be advised by submission of a revised DIS Form 553.

f. When a CSO determines that there is immediate danger of classified information being compromised or that security conditions in a facility are unsatisfactory to the degree that the FCL should be revoked, action shall be taken in accordance with paragraph 4-201.

g. If a FCL has been revoked on grounds pertaining solely to the physical elements of security, the LOC issued for the personnel of the facility need not be revoked. In such cases, however, the individuals concerned shall not be furnished access to additional classified information. If corrective action is subsequently taken by the contractor to bring the facility up to the standards prescribed in the ISM, the CSO may grant a new FCL. If such action is taken within 6 months from the time of revocation of the FCL, it will be

unnecessary to issue new LOC's for the personnel of the facility. If the time lapse is more than 6 months, the investigations of the personnel concerned shall be brought up to date and new LOC issued.

h. When a FCL has been granted and any information develops which indicates that the facility should no longer be eligible for the FCL, the activity discovering such information shall immediately report the facts to the CSO. In coordination with interested UA's, the CSO shall take necessary action to safeguard the classified material and, if appropriate, proceed to revoke the FCL in accordance with paragraph 4-201. The Director, DIS, ATTN: Deputy Director (Industrial Security) shall be advised and where indicated, a full report shall be made to the DUSD(P), ATTN: DSP&P. The DISCO shall be advised promptly of such action by submission of a DIS Form 553.

2-122 Appeals Not Authorized. In the following cases, denial or revocation of a FCL is taken exclusively by the DIS; appeals to the DUSD(P), ATTN: DSP&P, are not authorized:

a. cases involving research, development, and production of COMSEC or SENSITIVE COMPARTMENTED INFORMATION equipment or information;

b. cases involving denial or revocation of a FCL for a contractor or prospective contractor based on grounds of an overall security evaluation of unsatisfactory, or on conditions which constitute an immediate danger of compromise of classified information;

c. cases involving failure of the contractor to obtain a PCL for or to exclude a RFI; and

d. cases involving contractors listed in the "Consolidated List of Debarred, Ineligible, and Suspended Contractors," provided the CSO has taken the action required by paragraphs 2-111g and 2-118g.

2-123 Reprocessing of a Facility Security Clearance That Has Been Revoked.

a. If a FCL has been revoked for the reasons set forth in paragraph 2-121f, and the CSO considers that there are new circumstances which warrant granting a FCL, recommendations shall be made to the Director, DIS. On approval, a new FCL shall be granted by the CSO.

b. If a FCL has been denied or revoked as a result of action taken by DISCR and the CSO considers that there are new circumstances which warrant the granting of a FCL, recommendations shall be made through DISCO to the DUSD(P), ATTN: DSP&P. This procedure does not authorize the CSO to grant a FCL in such case, pending final action under the Industrial Personnel Security Clearance Program.

PART 2. U.S. FACILITIES THAT ARE FOREIGN OWNED, CONTROLLED, OR INFLUENCED

2-200 Application. This part establishes the policy concerning the clearance of facilities under FOCI; provides criteria to be considered for

determining whether facilities located in the U.S., Puerto Rico, and U.S. possessions or trust territories are under FOCI; prescribes procedures for the clearance of facilities determined to be under FOCI; and outlines responsibilities in FOCI matters.

2-201 General Policy.

a. A facility shall be considered under FOCI when a reasonable basis exists to conclude that the nature and extent of FOCI is such that foreign dominance over the management or operations of the facility may result in the compromise of classified information or impact adversely the performance on classified contracts.

b. A facility that is owned, controlled, or influenced by a foreign national or a commercial or governmental entity from a Communist country or a country overtly hostile to the U.S. will not be eligible for a FCL.

c. A facility that is owned, controlled, or influenced by foreign interests other than those included in b above may be eligible for a FCL, provided action can be taken to negate effectively or reduce associated FOCI risks to an acceptable level.

d. Contractors cleared or being considered for a FCL under this part who require release of COMSEC information are subject to the provisions contained in the "National Communications Security Committee Policy Number 2" (NCSC-2).

2-202 Factors. The following factors shall be considered in determining whether a business or educational entity is under FOCI:

a. foreign interest ownership or beneficial ownership of 5 percent or more of the organization's securities;

b. ownership of any foreign interest in whole or in part;

c. management positions held by foreign interests such as directors, officers, or executive personnel;

d. foreign interests control or influence or are in a position to control or influence the election, appointment, or tenure of directors, officers, or executive personnel of the organization;

e. contracts, agreements, understandings, or arrangements with foreign interests;

f. indebtedness to foreign interests;

g. any income derived from Communist countries, countries overtly hostile to the U.S., or income in excess of 10 percent of gross income from other foreign interests;

h. 5 percent or more of any class of the entity's securities are held in "nominee shares," in "street names," or in some other method that does not disclose the beneficial owner of equitable title;

1. interlocking directors with foreign interests; or

j. any other factor that indicates or demonstrates a capability on the part of foreign interests to control or influence the operations or management of the business organization concerned.

2-203 Procedures.

a. If any of the factors outlined in paragraph 2-202 above are present, the CSO shall review the case to determine the relative significance of each factor in assessing the firm's initial or continued eligibility for a FCL. The CSO may be delegated authority to grant or continue a FCL when one or more of the following circumstances are present, provided there is a favorable finding by the Director of Industrial Security:

(1) interlocking directorates involving firms located in non-Communist countries, provided that a general security of information agreement (GSOIA) exists with the country involved;

(2) if licensing, patent, sales, or trade secret agreements exist or are entered into with any foreign interest, including a subsidiary of the contractor, and if the contractor's SPP includes adequate provisions to ensure that RFI's who are parties to such agreements shall be denied access to all classified records, information, and material, and to controlled areas -- in all such cases the contractor shall be informed of the obligation to comply with the State Department's ITAR (reference (1)) as it pertains to such agreements with foreign interests;

(3) if income from Communist countries does not exceed 5 percent of gross income, and income from other countries does not exceed 20 percent of gross income;

(4) if the contractor has ownership in foreign subsidiaries or affiliates that are located in non-Communist countries;

(5) if information disclosed regarding securities held in "nominee shares" and "street names" reveals no indication of foreign beneficial ownership; or

(6) if indebtedness to foreign interests does not exceed 5 percent of current assets.

b. If the CSO determines that the firm may be ineligible for a FCL or that additional action may be necessary to nullify or negate the effects of FOCI, the firm promptly shall be advised and requested to submit a plan of action to preclude foreign interests from access to classified information. Assistance shall be provided to the facility in formulating such a plan in accordance with paragraph 2-204 below. In addition, management shall be advised that failure to submit the requested plan within the

prescribed period of time will result in termination of FCL processing action or initiation of action to revoke an existing FCL, as applicable.

c. Whenever the CSO is unable to resolve the FOCI factors present or has not been delegated authority to grant or continue a FCL as provided for in paragraph a above, the facility case file shall be referred to the Director, DIS, ATTN: Deputy Director (Industrial Security), for determination as to eligibility for a FCL. The facility case file shall be documented to set forth the FOCI factors present, as well as the facility's proposed plan of action 7/ to reduce effectively the associated FOCI risks to an acceptable level. The case file also shall contain the CSO's evaluation and recommendation and, as appropriate, an opinion of legal counsel. If legal advice is required to process the case, the Director of Industrial Security should consult with the Office of Counsel of the DCASR servicing the area. Cases in which a foreign interest has acquired a majority of the voting stock of a cleared U.S. firm will be reported immediately to the Director, DIS, ATTN: Deputy Director (Industrial Security), concurrent with invalidation of the FCL in accordance with paragraph 2-118k above.

d. On receipt of a referral from the CSO, the Director, DIS will cause a review to be made of the case. If, after such review, it is determined that unacceptable risk associated with FOCI is present, and that the facility's proposed plan to negate or eliminate such risk is inadequate, the Director, DIS shall advise the facility, through the CSO, of the measures required to become eligible for a FCL. The facility shall be advised that failure to adopt the recommended or other acceptable measures shall preclude final determination of the facility's eligibility for a FCL and will result in denial or revocation of the FCL. If, however, the facility's proposed plan is viewed as adequate by the Director, DIS, or the modifications suggested by DIS are subsequently accepted by the facility, the Director, DIS shall determine the facility to be eligible for a FCL.

e. In the event of an adverse determination by the Director, DIS, the facility shall be advised that the decision may be appealed in writing to the Deputy Under Secretary of Defense (Policy) (DUSD(P)), ATTN: Director, Security Plans and Programs, whose decision in such matters shall be final.

2-204. Assistance. Whenever requested by the facility, or on receipt of the report required by paragraph 6a(4)(f), ISM, the CSO or the Deputy Director (Industrial Security), HQ DIS shall provide the facility in writing

7/ A facility's proposed plan of action may consist of one of the methods prescribed by 2-205 below, or any combination thereof, as appropriate. It may also consist of measures that provide for the physical or organizational separation of the facility component performing the classified work, modification or termination of agreements with foreign interests, diversification or reduction of foreign source income; assignment of specific security duties and responsibilities to board members; formulation of special executive-level security committees to consider and oversee classified matters; and other actions to negate or reduce FOCI to acceptable levels.

with the DoD policy regarding FOCI and will consult with the facility as needed to provide additional advice and guidance regarding the facility's proposed action plan. Documents relating to these discussions and reports made pursuant to the foregoing are presumptively proprietary when appropriately designated by the facility and shall be protected from unauthorized disclosure and handled on a strict need-to-know basis. When such reports are submitted in confidence, they shall be marked "FOR OFFICIAL USE ONLY" (FOUO). DoD Directive 5400.7 (reference (1)) contains exemptions which, to the extent applicable to FOUO records, may be invoked to withhold them from public disclosure.

2-205 Methods to Negate or Reduce Risk in Foreign Ownership Cases.

Under normal circumstances, foreign ownership of a U.S. firm under consideration for a FCL becomes a concern to the DoD when the amount of foreign owned stock is at least sufficient to elect representation to the U.S. firm's board of directors, or foreign interests are otherwise in a position to select such representatives (equivalent equity for unincorporated business enterprises). Foreign ownership which cannot be so manifested is not, in and of itself, considered significant and, therefore, shall not be considered as the sole criteria for processing under this paragraph 8/.

a. Board Resolution. When the amount of stock owned by the foreign interest is sufficient to elect representation to the board or an agreement exists whereby the foreign interest is permitted representation on the board, the effects of foreign ownership will ordinarily be mitigated by a resolution of the board of directors whereby the cleared firm recognizes the elements of FOCI and acknowledges its continuing obligations under the DD Form 441. The resolution shall identify the foreign shareholders and their representatives, if any, and note the extent of foreign ownership, including a certification that the foreign shareholders and their representatives will not require, will not have, and can be effectively excluded from access to all classified information in the possession of the cleared facility, and will not be permitted to occupy positions that may enable them to influence the organization's policies and practices in the performance of classified contracts. Copies of such resolutions shall be furnished to all board members and principal management officials. In addition, the substance of the foregoing resolutions shall be brought to the attention of all cleared personnel by publication in the firm's SPP. An annual certification shall be provided to the CSO acknowledging the continued effectiveness of the resolutions. Compliance with the resolutions shall be verified during periodic security inspections. There are circumstances when it may become necessary for the board of directors to adopt further resolutions and take additional administrative actions in order to assure the U.S. Government that the existing FCL remains clearly consistent with the national interest. The following criteria also shall

8/ Instances involving less significant foreign stockholdings are analyzed to assess source and to determine possible significance when considered in conjunction with other aspects of foreign involvement that may be present in a particular case.

be satisfied in order for a board resolution to be used as the sole method required to negate or effectively reduce the risk of compromise arising from foreign ownership within the levels prescribed herein.

(1) Identified U.S. interests own a majority of the stock, a foreign interest is not the largest single shareholder, and the nature and distribution of the minority stockholdings and the composition and structure of management do not permit foreign interests to control or dominate the business management of the U.S. firm.

(2) The chairman and chief executive officer of the U.S. firm are U.S. citizens.

b. Voting Trust Agreement. A voting trust agreement is an acceptable method to eliminate risks associated with foreign ownership when a foreign interest owns a majority of the voting securities of the U.S. firm or, if less than 51 percent foreign owned, it can be reasonably determined that the foreign stockholders or their representatives are in a position to effectively control or have the dominant influence over the business management of the U.S. firm. Under this arrangement, the foreign stockholders shall transfer legal title of foreign-owned stock to the trustees. The voting trust arrangement unequivocally shall provide for the exercise of all prerogatives of ownership by the trustees with complete freedom to act independently without consultation with, interference by, or influence from foreign stockholders. Except, however, the trust agreement may limit the authority of the trustees by requiring that approval be obtained from the foreign stockholder(s) with respect to: (i) the sale or disposal of the corporation's assets or a substantial part thereof; (ii) pledges, mortgages, or other encumbrances on the capital stock that they hold in trust; (iii) corporate mergers, consolidations, or reorganization; (iv) the dissolution of the corporation; and (v) the filing of a bankruptcy petition. The trustees shall assume full responsibility for the voting stock and for exercising all management prerogatives relating thereto in such a way as to ensure that the foreign stockholders, except for the approvals just enumerated, shall be insulated from the cleared facility and continue solely in the status of beneficiaries. The facility shall be organized, structured, and financed so as to be capable of operating as a viable business entity independent from the foreign stockholders. The certification and visitation provisions of paragraphs 2-206 and 2-207 below are required under this arrangement. There shall be three trustees, and at least one shall become a member of the board of directors. In addition, trustees shall be:

(1) responsible U.S. citizens residing within the U.S., who are capable of assuming full responsibility for voting the stock and exercising the management prerogatives relating thereto in such a way as to ensure that the foreign stockholders shall be effectively insulated from the cleared facility,

(2) completely disinterested individuals with no prior involvement with either the facility or the corporate body in which it is located, or the foreign interest, and

- (3) eligible for and issued a PCL to the level of the FCL.

When a vacancy occurs, a successor trustee shall be appointed by the remaining trustees. Before being accepted as trustees by the Director, DIS, the trustees shall be advised, in writing, by the CSO of the duties and responsibilities they are undertaking on behalf of the U.S. Government to insulate the cleared facility from the foreign interests. Moreover, the trustees shall indicate, in writing, their willingness to accept this responsibility.

c. Proxy Agreement. Under this arrangement, the voting rights of stock owned by foreign interests are conveyed to the proxy holders by means of an irrevocable proxy agreement. Legal title to the stock remains with the foreign interests. All other provisions of the voting trust as applies to trustees and the terms of the agreement shall apply to the proxy holders in the case of a proxy agreement. Conditions for consideration of use are the same as required for the above.

d. Reciprocal Clearance. The DoD has entered into reciprocal industrial security agreements with certain of its allies. These agreements establish arrangements whereby a contractor facility located in either signatory country, which is under the ownership, control, or influence of an entity from the other country may be declared eligible for access to classified information. This arrangement also provides for the clearing of foreign nationals who occupy a position required to be cleared in connection with the issuance of a FCL. FCL action is based on the receipt of an assurance from the government of the country from which the FOCI emanates that the parent firm has been cleared to the necessary level under that government's security laws and procedures. Since clearance actions in such cases rely, in part, on the investigative and clearance procedures of the other signatory government, such reciprocal agreements are negotiated only with countries whose security laws and procedures are substantially equivalent to those of the U.S. If a facility is to be processed for a reciprocal FCL, the procedures outlined in paragraph 2-117 above shall be followed. A reciprocal FCL may be granted upon satisfaction of the following criteria and conditions:

(1) there is a reciprocal industrial security agreement with the foreign government concerned;

(2) a foreign business entity enjoys majority or controlling ownership of the U.S. firm, or a foreign interest is otherwise in a position to effectively control or have the dominant influence over the business management of the U.S. firm; and

(3) the facility does not require access to classified information which is not releasable to the foreign government from which the ownership stems.

e. Special Security Agreement.

(1) This arrangement may be considered for use when the foreign interest owns a majority of the voting stock of a U.S. firm or, if less than a majority is owned, such stockholdings are sufficient to conclude

reasonably that the foreign shareholders or their representatives are in a position to effectively control or have the dominant influence over the business management of the U.S. firm, and the foreign shareholders elect to retain control or dominance of operations and management.

(2) Eligibility for processing under this paragraph also requires a UA and OSD determination that issuance of a FCL will serve the national interest. Such determinations along with sufficiently detailed supporting justification, shall be forwarded to the DUSD(P), ATTN: Director, Security Plans and Programs, for confirmation in coordination with appropriate OSD staff elements. The authority to make this determination shall not be delegated below the Assistant Secretary or comparable level of the UA concerned or his or her designee. Following confirmation of national interest considerations ^{9/} and coordination with non-DoD components, as appropriate, DUSD(P) will direct DIS to initiate development of a special security agreement and inform DIS regarding any prohibited categories of classified information (see paragraph 2-117a), access to which is not required by the U.S. firm, and which will not be authorized for release after issuance of the FCL. Categories of such information not approved for release, if any, shall be reflected on DIS Form 553, DIS FL 381-R, and DISCO Form 560.

(3) The special security agreement concept may be considered as a fully acceptable alternative to voting trust or proxy agreement arrangements, provided the ownership stems from a country in which the U.S. has entered into a formal reciprocal security agreement and all personnel required to be cleared in connection with the FCL are U.S. citizens, except that the facility shall normally be ineligible for a TOP SECRET FCL. This arrangement may also be considered when the ownership stems from countries in which the U.S. has not entered into formal reciprocal arrangements, provided a GS0IA or other similar bilateral security agreement exists with the country concerned, all personnel required to be cleared in connection with the FCL are U.S. citizens, and the FCL is limited to the CONFIDENTIAL level.

(4) This agreement ordinarily shall include annual FOCI meetings with the principals, visitation agreements (appropriately modified), assignment of specific security duties and responsibilities to board members, formulation of special executive-level security committees to consider and oversee classified matters, and the execution of any board resolutions deemed necessary. A facility under FOCI may be granted a FCL under this arrangement only when the terms and conditions of the special security agreement, in conjunction with ISM requirements, are determined to reasonably and effectively preclude the unauthorized disclosure of classified information to foreign interests. The measures taken to accomplish necessary security safeguards will depend upon the nature and extent of FOCI in each particular case. Accordingly, each such special security agreement is considered unique and its contents shall be developed and tailored on a case-by-case basis, wholly dependent on the facts and circumstances present in each instance. The special security agreement shall generally prescribe

^{9/} The NSA, as the Executive Agent for COMSEC, enjoys final approval authority regarding the release of COMSEC information to a facility operating under special agreement arrangements.

responsibilities, obligations, limitations, and other security safeguards and mechanisms concerning personal, physical, and organizational aspects deemed necessary by the parties to the agreement. The U.S. firm, the foreign interests, and the DoD shall be parties to the agreement.

(5) The granting of a FCL under this arrangement, or any request for an exception to the policy prescribed herein, requires the approval of the DUSD(P).

2-206 Visitation Agreements. In every case where a voting trust agreement, proxy agreement, or special security agreement is employed to eliminate risks associated with foreign ownership, a visitation agreement shall be executed between the facility, the foreign interest, the CSO, and as appropriate, trustees, proxy holders, or other designated individuals, hereinafter referred to collectively as trustees. Visitation agreements shall identify who may visit, for what purposes, when advance approval is necessary, and the approval authority. The trustees shall have approval authority. The facility shall submit individual requests to the approval authority for each visit. The visitation agreement shall provide that, as a general rule, visits between the foreign stockholder and the cleared U.S. firm are not authorized; however, as an exception to the general rule, the trustees, may approve such visits in connection with regular day-to-day business operations pertaining strictly to purely commercial products or services and not involving classified contracts.

2-207 Certification and Compliance. At the inception of any method, agreement, or similar arrangement entered into pursuant to paragraph 2-205 above, and at least once each year thereafter, representatives of the CSO, HQ DIS, the trustees, proxy holders, facility management, or, as appropriate, other designated individuals, and if requested, the foreign interests, shall meet to review the purpose of the pertinent arrangement and to establish a common understanding of the operating requirements and how they will be implemented within the firm. These FOCI reviews will be aimed expressly at ensuring compliance with all board resolutions, special controls, practices, and procedures established to insulate the facility from the foreign interest generally, and to discuss matters pertaining to the compliance or acts of noncompliance with the terms of voting trust, proxy, or special security agreements specifically. These reviews also provide the opportunity for DIS to furnish the principals with any necessary guidance or assistance regarding problems or impediments associated with the practical application or utility of the approved arrangement, such as foreign disclosure determination delays and non acceptance of visit requests. In addition, at the end of each year of operation, the trustees, shall submit to the CSO an annual implementation and compliance report. Any indication of noncompliance must be explained, in writing, by the firm for evaluation by the CSO. Failure on the part of the U.S. firm to ensure compliance with the terms of the applicable arrangement in the best interests of the U.S. Government, may constitute grounds for termination of the DD Form 441 and revocation of the FCL.

2-208 Effects of This Part on Prior Facility Security Clearances. U.S. firms granted FCL's under previous policy will not be affected by this part. Such firms may, as appropriate, however, request modification of existing arrangements in accordance with this part.

Part 3. PERSONNEL SECURITY CLEARANCES AND DENIALS FOR CONTRACTOR PERSONNEL

2-300 Application. This part establishes policy and procedures for the granting of PCL's for U.S. contractor personnel, including immigrant aliens; security assurances for U.S. citizens in countries with which the U.S. has entered formal reciprocal arrangements and security assurances for citizens of these countries who are employees of U.S. contractors; and for the granting of access authorizations to NATO classified information. In addition, this part sets forth procedures for the recommendation for suspension, revocation, or denial of PCL's.

2-301 Security Clearances for Personnel

a. General. A PCL is an administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the PCL being granted. A PCL granted by the DoD or by a contractor for access to classified information is valid for access to classified information of the same or lower category. A PCL (or an interim PCL) is required for contractor personnel prior to granting them access to classified information. Personnel shall not be cleared for access to classified information of a higher category than the level of security clearance of the facility at which they are employed except for.

(1) consultants, as provided for in paragraph 2-106 of this regulation, and

(2) employees of a MFO (including those employed or physically located at uncleared facilities) who (i) require access to a higher category of classified information in connection with the performance of their duties at another cleared facility or at a government installation, or (ii) are transferred to an uncleared facility or to a facility with a lower level of clearance within the MFO, provided the contractor desires to retain the LOC at the higher level so it will be available in the event the individual is transferred back to a facility at which the clearance will be needed. A clearance granted under this authority shall not be of a higher category than the PCL of the HOF or appropriate PMF of the contractor, and the LOC will be issued or forwarded to the HOF or PMF.

b. Interim Clearances. In an emergency situation, in order to avoid crucial delays in precontract negotiations or contract negotiations, on performance of a contract or under the conditions described in paragraphs 2-307h, 2-308e(2), 2-308g(2), or 2-111b(4) of this section, a PCL based on lesser investigative requirements as prescribed by this regulation may be granted on a temporary basis, pending the completion of the full investigative requirements. If, on review of the DD Form 48 or DD Form 49 it is apparent that the full investigative requirements for the level of PCL requested cannot be completed to meet prescribed standards, an investigation to satisfy lesser interim investigative requirements shall not be initiated nor shall an interim PCL be granted. The facility and the contracting officer shall be notified to this effect. When a clearance based upon the lesser standards is authorized, this shall be identified as an interim PCL. An interim PCL shall not be

granted unless a request for investigation of a type required to satisfy final clearance requirements has been initiated. When an interim PCL has been granted and derogatory information is subsequently developed during the course of the investigation, the Director, DISCO may withdraw the interim clearance, pending the completion of the investigation. Notice of this action shall be furnished to the facility. Such withdrawal will not be construed as a denial or revocation of the clearance and referral of the case to the DISCR, OGC, OSD for processing is not required prior to the completion of the investigation; however, the DISCR, OGC, OSD shall be notified promptly of all such withdrawals of interim clearances and the basis therefor.

c. Invalid and Void Clearances. When a clearance is issued as a result of administrative error or to an individual not eligible for clearance, it is invalid and void from the date of issue. When it has been determined that an invalid and void clearance has been issued, the Director, DISCO shall withdraw such a clearance. The Director, DISCO shall apprise the contractor that the withdrawal action is taken without cause or prejudice against the individual. The contractor shall be requested to return the LOC. A copy of such official notice to the contractor shall be provided the CSO and the Deputy Director (Industrial Security), HQ DIS.

d. Administrative Termination of a Clearance on the Basis of Expressed Conviction. A contractor employee who is being processed for an industrial PCL or is currently cleared must have a need for access to classified information in order for a clearance to be processed or continued. Employees who have submitted their DD Forms 48 or 49, but who aver on the form, or otherwise make it known that they will not work on a classified contract or perform in a capacity requiring access to classified information for any reason, cannot be considered either as bona fide candidates for clearance or individuals whose continued clearances are in the best interest of the government, notwithstanding the formal initiation of clearance requests or the issuance of a clearances. Such a reservation on the part of employees negates the requirement for their clearances because they will not, in fact, have access to classified information. On receipt of a report by the contractor, DISCO will correspond with the employees to obtain verification of such objections and elicit in writing from the employees their individual positions relative to the following questions.

(1) Will these applicants perform duties on a classified defense contract if so assigned by their employer, even though the contract will directly further the military capability of the U.S.?

(2) Will such applicants follow all security directives and instructions, and otherwise fulfill all of their personal responsibilities concerning the safeguarding of classified information?

(3) Will such applicants report to the contractor or to government security representatives any effort by an unauthorized person or persons to elicit any classified information from them?

Should DISCO be unable to elicit a satisfactory response from the employees through correspondence, DISCO shall request interviews of the employees in order to resolve the matter. When verified, the clearance requests or existing clearances will be administratively terminated by the Director or

Deputy Director, DISCO, without prejudice to the individuals concerned, and the contractor and the employees will be advised of the termination.

2-302 Defense Industrial Security Clearance Office.

a. The DISCO is responsible for initiating investigation, issuing clearances, maintaining clearance records, and preparing recommendations to the DISCR, OGC, OSD for suspension, revocation, or denial of clearance, when applicable, with respect to PCL's for all contractor personnel falling within the scope of this regulation.

b. The DISCO will receive requests for PCL's from all cleared contractor facilities. Each request will be reviewed for necessity, completeness, and accuracy. The DISCO will, following acceptance of the request, initiate a request for a personnel security investigation.

c. All actions having a bearing on contractor PCL's will be recorded in the PSCF.

d. Existing LOC's are valid during the periods specified in paragraph 2-307b, or until suspended, revoked (see paragraph 2-320), or administratively terminated, without prejudice to the individual (see paragraphs 2-310 and 2-402). Adverse information concerning the subject of the LOC shall be reported promptly to DISCO.

e. Except as outlined below, LOC's shall be issued to the facility at which individuals are employed or physically located. The exceptions, applicable only in the case of a MFO, are as follows.

(1) This includes situations as described in paragraph 20d, ISM, where the employees, in connection with the performance of their duties at other cleared facilities or a government installation: (i) requires access to a higher category of classified information than the FCL of the facility at which they are employed or physically located, or (ii) when they are employed or physically located at an uncleared facility. In such cases, the LOC's are issued to the HOF or appropriate PMF of the MFO, and they may not be for access to a higher category of classified information than the level of the FCL of the HOF or PMF.

(2) When contractors elect to have LOC's for all employees issued to the HOF or PMF at which the individuals are employed or physically located, contractors shall include in their SPP this procedure and forward the SPP to the CSO. On receipt of the SPP, the CSO shall review the SPP, coordinate with DISCO, and notify the contractors of the adequacy of the SPP. The CSO may, at its option, visit the uncleared location to evaluate the effectiveness of personnel security administration as it relates to briefings, foreign travel, termination statements, notifications, and so on. The SPP shall identify: (i) each facility of the MFO, or (ii) each facility of the MFO that is located within the geographical or functional area for which the PMF is administratively responsible.

(3) This also includes situations as described in paragraph 20j, ISM, when individuals are required to be cleared in connection with the HOF security clearance and their primary place of work is at another

facility of the MFO. In this case, LOC's are issued to both the HOF and the facility where the individuals are primarily employed. An appropriate notation shall be included on the DISCO Form 560.

2-303 Special Status of Certain American Indians Born in Canada. American resident members of the Six-Nation Confederacy or the Sovereign Nation of Iroquois Indians (Seneca, Cayuga, Onondaga, Oneida, Tuscarora, and Mohawk tribes) born in Canada who possess at least 50 percent tribal blood are eligible for clearance for access to classified information in the same manner as any other immigrant alien without, however, being required to possess an immigrant visa for permanent residence. The Immigration and Naturalization Service, Department of Justice, and the Bureau of Indian Affairs, Department of the Interior, shall be checked, in addition to the investigation prescribed by paragraph 2-319 of this part, for registration as aliens and to determine under the provisions of the Immigration and Nationality Act of 1952 (reference (kk)) whether the individual has 50 percent tribal (Indian) blood.

2-304 Transfer of Personnel Between Facilities of a Multiple Facility Organization. The following procedure shall apply when an employee, who has been granted a PCL by the DoD, is transferred within a MFO, and the contractor requires the employee to have access to classified information in the performance of his or her new duties.

a. The DISCO, having been notified by the contractor of the employee's transfer, shall annotate the DISCO Form 560 to show the employee's new place of employment.

b. The individual concerned shall not be requested to submit DD Form 48, DD Form 49, or (FD Form 258) "Applicant Fingerprint Card," unless a higher level of clearance is required at the gaining facility or there is information which indicates that the granting of a clearance might not be clearly consistent with the national interest.

c. A PCL transferred under the provisions of this paragraph may be of a higher security level than the PCL of the gaining facility (see paragraph 2-301a).

2-305 Processing of a Hostage Case.

a. A hostage case is defined as one falling within the range of subsection V K of DoD Directive 5220.6 (reference (ll)). The situation described in subsection VK comes about when, with respect to the relatives of the applicant or of the spouse, there are: "any facts or circumstances which furnish reason to believe that the applicant may be subjected to coercion, influence, or pressure which may be likely to cause action contrary to the national interest. Such facts or circumstances may include the presence of a close relative, friend, or associate in a nation whose interests may be inimical to the interests of the U.S., or in satellites or occupied areas of such a nation. Close relatives include parents, brothers, sisters, offspring and spouse."

b. The following procedures shall apply when a contractor, under the provisions of paragraph 24b(5), ISM, submits a hostage case to DISCO for further evaluation and determination of continued eligibility for access to CONFIDENTIAL information. The DISCO shall request that:

(1) a NAC be conducted;

(2) the scope of the investigation be expanded, as appropriate, to resolve the allegation that the individual might act contrary to the national interest because of coercion or pressure due to former residence in, or having relatives in Communist countries; and

(3) a personal interview by the investigative activity be held with the individual to determine the extent of the hostage situation, to provide guidance, and to encourage reporting of any attempted coercion.

c. In all other hostage cases, DISCO shall:

(1) request the investigation prescribed in paragraph 2-308,
and

(2) request the additional actions prescribed in paragraphs b(2) and (3) above.

d. On completion of the action prescribed in paragraphs b or c above, DISCO shall, if clearly consistent with the national interest, issue to the contractor a DISCO Form 560 for the individual concerned. If such determination cannot be made in the case, the procedures outlined in paragraph 2-320 of this regulation shall apply.

2-306 Processing of a Representative of a Foreign Interest Case.

a. Special requirements are established in paragraph 20k, ISM, for submission of a request for clearance on a RFI including those individuals who are presently cleared or those individuals who become RFI's while in the process of being cleared. RFI's are not eligible for PCL's if one of the following conditions exists.

(1) The foreign interest involves a Communist country or a citizen, firm, or other entity of a Communist country.

(2) The individuals' work as representatives of a foreign interest could create a potential conflict of interest situation vis-a-vis their work for the contractor if PCL's were to be issued for them. (A potential conflict of interest situation is considered to exist when an individual's technical or scientific endeavors on behalf of a foreign interest are similar to his or her technical or scientific endeavors on behalf of the U.S. contractor; for example, the individual is performing services as a consultant to a foreign government and to a U.S. contractor involving the same general scientific or technical discipline).

(3) The individuals are not U.S. citizens or U.S. nationals. This general exclusion is not applicable to citizens who are of countries with

which the U.S. has entered into formal reciprocal arrangements and who are eligible for or have been previously granted reciprocal clearances in accordance with the provisions of paragraph 31, ISM. Where it is determined that any of the foregoing conditions exist, the case shall be referred to the Director DIS, ATTN: Deputy Director (Industrial Security). If the Director, DIS concurs in the DISCO determination that any of the foregoing conditions exist, DISCO will be advised to notify the contractor that pursuant to paragraph 20k, ISM, the individual is not eligible for a PCL, and any previously issued PCL shall be administratively withdrawn.

b. In cases where a RFI is eligible to be processed for or continues to possess a PCL, DISCO shall review the clearance application with particular attention to the statement of full disclosure submitted pursuant to paragraph 20k, ISM, to determine the security significance of the foreign affiliation. If DISCO determines the circumstances of the foreign affiliation or other considerations in the case raise a question that the individual may be subject to coercion, pressure, or otherwise influenced or placed in a position which could jeopardize the security of classified information or be otherwise contrary to the national interest, DISCO shall initiate an investigation to obtain all the facts of the matter. This shall include investigation to verify the information furnished by the applicant in accordance with paragraph 20k, ISM, which describes the foreign affiliation. It should be determined whether or not the foreign entity is under Communist ownership, control, or influence. In addition, the nature of the business or activity of the foreign entity should be determined. For example, the report should indicate and fully describe the nature of the business and products of the foreign entity, in order that a determination can be made as to whether the circumstances of the foreign affiliation furnish reason to believe that the individual may be subject to coercion, pressure, or otherwise influenced to act contrary to the national interest. Normally, the necessary information with respect to the foregoing can be obtained from the U.S. Commercial Attache in the country concerned. On completion of the investigation, DISCO shall evaluate the case. It is then determined that any of the conditions described in paragraph a above, are present, the case shall be referred to the Director DIS, ATTN: Deputy Director (Industrial Security). On the other hand, if the conditions described in paragraph a above are not present, but in light of the individual's status as a representative of a foreign interest and all of the other information available, the Director, DIS determines that access would not be clearly consistent with the national interest, the case shall be referred to DISCR, OGC, OSD, in accordance with paragraph 2-320.

c. In those cases involving a transfer, conversion, or concurrent clearance, DISCO shall review the clearance application with particular attention to the statement submitted in connection with the request pursuant to paragraph 20k, ISM. If, on the basis of this review DISCO determines that an investigation is warranted because of the circumstances in the case, an investigation to include a NAC and the coverage described in paragraph b above shall be initiated. In such cases, if otherwise appropriate, the LOC shall be issued. The investigation as prescribed above shall be initiated as a post-transfer action. On completion of the investigation, the case shall be evaluated to determine if revocation action is required. When appropriate, such action will be taken in accordance with paragraph 2-320 of this regulation. If the investigation indicates the case falls into one of the

categories described in paragraphs a(1), (2), or (3) above, the case shall be referred to the Director, DIS, ATTN: Deputy Director (Industrial Security).

2-307 Responsibility for Effecting Contractor Personnel Security Clearances.

a. The DISCO shall be responsible for the clearance of such contractor employees as may be required for the performance of any classified contact, except as provided for by paragraph 1-306, or those CONFIDENTIAL clearances which shall be accomplished by the contractor. The DISCO shall complete all actions necessary for the granting of a PCL and will determine whether to grant the clearance or refer the case to the DISCR, OGC, OSD, in accordance with paragraph 2-320. Subject to the provisions of paragraph 2-320, any prior industrial PCL actions that may have been accomplished by any military department, provided these actions meet the investigative basis prescribed in this regulation, shall not be duplicated, but shall be accepted by DISCO.

b. LOC's previously issued to a facility remain valid as long as an individual is continuously employed by that facility and during any period of reemployment with any facility of the same organization which commences within 12 months after the cessation of prior employment, unless otherwise revoked or administratively withdrawn. In addition, when an employee is granted a leave of absence, it shall not be considered as an interruption or discontinuance of employment so long as it does not exceed 12 months.

c. Whenever an individual has been authorized access to classified information within a facility and is subsequently employed by another facility and the procedures established by paragraphs 26e or g, LSM, are followed, DISCO shall issue a LOC based on the previous investigation, provided the following conditions are met.

(1) The individual is still employed by another contractor or there has been a lapse of not more than 12 months between termination of employment and submission of the request for clearance.

(2) The investigative basis upon which the LOC was issued satisfies the requirements of paragraph 2-308.

(3) The new LOC issued for the individual shall not authorize access to information of a higher classification than the of the facility employing him or her, except as provided for in paragraph 2-301a.

(4) When individuals have terminated their employment with the facility where they have been granted PCL's or when individuals also continue to be employed by their other employers in a capacity requiring access to classified information, DISCO shall ascertain from the PSCF that there exists no information which would reflect on the advisability of granting clearances in accordance with this paragraph. This includes an evaluation of information reported under the provisions of paragraph 6a(1) or 6b(1), LSM. However, unless such information is serious enough to support interim suspension actions pursuant to paragraph 2-320, the clearances shall be transferred without delay. When there is adverse information which does not warrant an interim action, but does require action in accordance with paragraph 2-320b, DISCO shall initiate the appropriate action concurrent with the transfer of the clearance.

(5) The DD Form 48-3, "Department of Defense Personnel Security Questionnaire (Updating)," is submitted by the contractor. The individual concerned shall not be required to submit a fully executed DD Form 48, DD Form 49, or FD Form 258 to accomplish the above action unless the basis of the previous clearance does not satisfy the investigative requirements of paragraph 2-308, ISM, or there is information which indicates that the granting of a clearance might not be clearly consistent with the national interest.

(6) An exception to the requirement for submission of a DD Form 48-3 to obtain a concurrent clearance can be made when an OODEP of a parent company becomes concurrently an OODEP of a subsidiary, or when an OODEP of a subsidiary becomes concurrently an OODEP of the parent company. He or she can be issued a concurrent clearance without submission of a DD Form 48-3 provided the new clearance being requested is not of a higher level than the current clearance. In these cases, the contractor will follow the procedures set forth in paragraph 26g, ISM. Any action by the government to suspend or revoke a concurrent clearance shall be equally applicable to all such clearances issued for the consultant or OODEP and the employers concerned will be so notified.

(7) When a cleared employee of a collocated cleared facility as described in paragraph 72c, ISM, is transferred to another collocated facility, DISCO, on receipt of the DISCO Form 562, will issue a DISCO Form 560 to the gaining facility provided there is no break in employment of more than three (3) working days.

d. When a contractor employee terminates employment prior to the completion of an investigation, such investigation may be terminated if this action is advantageous to the government. Should the investigation be completed only because it is considered more economical to do so, the results of the investigation will be recorded in the PSCF. If the case has been referred to the DISCR, OGC, OSD, they shall be notified immediately of the termination of the employee's employment.

e. If DISCO or the investigative agency determines that the full investigation cannot be completed to meet the standards prescribed for the level of clearance being granted, the investigation shall be stopped at that point. The DISCO shall be notified promptly and shall, in turn, notify the facility.

f. In all cases other than those described in paragraphs d and e above, a PCL action shall continue until the applicant's eligibility for a PCL has been determined by appropriate authority, unless it is established that the clearance is no longer required or the applicant has not requested the continued processing of his or her case under the provisions of section IV E of DoD Directive 5220.6 (reference (11)).

g. On receipt of an application for an interim CONFIDENTIAL clearance submitted by the contractor in accordance with paragraph 26d, ISM, DISCO may issue an interim CONFIDENTIAL clearance as prescribed in paragraph 2-308g(1). Prior to issuing a clearance DISCO shall ascertain from the DCII and the PSCF that no derogatory information exists which could preclude granting an interim CONFIDENTIAL clearance.

h. Immigrant aliens who are not RFI's who reside permanently in the U.S., intend to become U.S. citizens as soon as becoming eligible to do so, and have been determined qualified pursuant to paragraph 2-327, may be processed for PCL's in accordance with requirements established by paragraph 2-308. The investigation shall be expanded to include an interview with applicants to obtain statements of full disclosure with respect to their national allegiance, determine their reasons for being in the U.S., their intent to reside permanently in the U.S., and an expression of their general attitude toward the U.S. vis-a-vis the country to which they owe national allegiance. An immigrant alien contractor employee who does not reside or does not intend to reside permanently in the U.S. and obtain U.S. citizenship is not a bona fide candidate for issuance or continuance of a PCL. The processing of a PCL or any existing PCL for such an immigrant alien shall be administratively terminated by DISCO without prejudice to the individual concerned. DISCO will notify the contractor and the employee of the administrative termination. Residence or assignment of cleared immigrant aliens outside the U.S., Puerto Rico, Guam, or the Virgin Islands, negates the basis on which the LOC was issued, and the LOC will be administratively terminated without prejudice by DISCO on receipt of contractor notification as outlined in paragraph 6b(6), ISM. Such individuals, on visits of 90 consecutive days or less within a 12-month period to foreign areas, are not considered to be assigned or be in residence outside the U.S. Visits in excess of 90 consecutive days duration shall invalidate any existing clearance.

2-308 Requirements for Security Clearances for Contractor Personnel. The actions requiring accomplishment with favorable results prior to granting LOC's to facilities are prescribed below for the various levels of PCL's. Except for those foreign nationals eligible to be processed for a clearance under paragraph 2-323, foreign nationals, as defined herein, are not eligible for PCL's under the provisions of this regulation. To be processed as an applicant and to be eligible for clearance, an immigrant alien must evidence an "Alien Registration Receipt Card" (Form No. I-151 or I-551) and be a resident of and intend to reside permanently in the U.S., Puerto Rico, Guam, or the Virgin Islands of the United States. *

a. LOC's will be issued to facilities, provided the minimum investigative requirements for each category of information as set forth below are met, and provided information is developed which is sufficient for determination that the individual is eligible to be an applicant and to justify a determination that the clearance of the applicant is clearly consistent with the national interest.

b. TOP SECRET Personnel Security Clearance.

- (1) For U.S. citizens, a BI is required.
- (2) Immigrant aliens may not be authorized.

c. Interim TOP SECRET Personnel Security Clearance.

(1) For U.S. citizens, an interim TOP SECRET PCL may be granted only in those special cases when it is necessary to clear the personnel to prevent crucial delay in precontract negotiations or the award or

performance of a contract. Special authorization as to the need for granting an interim TOP SECRET PCL shall, in each case, be obtained from the Head of the UA or his or her designated representative 10/. Prior to granting an interim TOP SECRET PCL, a NAC with favorable results shall be completed by the investigative agency pending the completion of the required BI.

(2) Immigrant aliens may not be authorized.

d. SECRET Personnel Security Clearance.

(1) For U.S. citizens, a NAC is required or, in the case of former military personnel eligible under paragraph 2-309a, an Entrance NAC is required.

(2) For immigrant aliens, a BI is required. When an immigrant alien is admitted to the U.S. for a permanent residence, there is established a presumption that there has been a change of national allegiance from the native country to that of the U.S. When an immigrant alien becomes eligible for citizenship but elects not to become a citizen, the presumption of primary national allegiance to the U.S. is placed in doubt. As part of each personnel security investigation for access to classified information the immigrant alien applicant shall be interviewed by the DIS to determine if the applicant owes primary national allegiance to the U.S. Effective 1 year from the date of this issuance, DISCO shall identify those cleared contractor immigrant alien employees who have been eligible for U.S. citizenship for at least 12 months. DISCO shall then request a DIS interview of the individual to determine if the individual owes primary national allegiance to the U.S. On receipt of the DIS report, DISCO shall administratively review the case to determine if it is clearly consistent with the national security to continue the clearance.

e. Interim SECRET Personnel Security Clearance.

(1) For U.S. citizens, the contracting officer of the UA may request DISCO to grant interim SECRET PCL's when it has been determined that performance of the full investigative requirements prior to granting access to SECRET information to an individual will result in crucial delay in precontract negotiations or the award or performance of a contract. Satisfactory review of the DD Form 48 and the files of the DCII pending completion of the NAC is authorized as a basis for an interim SECRET PCL. As an exception to the foregoing procedures, the CSO is authorized to approve the grant, by DISCO, of an interim SECRET PCL for alarm service personnel (when the service relates to the supplemental control requirements of paragraph 14, ISM) and personnel who require a clearance in accordance with paragraph 20e, ISM, when an emergency situation exists, which would render the facility incapable of adequately safeguarding classified material in its possession, and no contracting officer is available to approve the interim clearance request within the time required to negate the threat.

10/ Each UA shall keep DISCO currently advised of the officials who have been designated by the Head of the UA for this purpose.

(2) For U.S. citizens with prior industrial PCL's, an interim SECRET PCL may be granted to a U.S. citizen employee who previously has been issued a LOC for a final SECRET or TOP SECRET clearance when there has been a lapse in employment for more than 12 but within 25 months since termination of the employment for which the LOC was issued, provided the employee has been subsequently employed in a position requiring access to SECRET information. Prior to granting an interim SECRET PCL, DISCO shall: (i) obtain the contractor's certificate indicating the date the previous SECRET or TOP SECRET clearance was issued and by whom it was issued; (ii) conduct a satisfactory review of the DD Form 48 and the files of the DCII, and (iii) initiate a request for a current NAC. Special authorization as to the need for granting an interim SECRET PCL from the contracting UA is not required.

(3) Immigrant aliens may not be authorized.

f. CONFIDENTIAL Personnel Security Clearances.

(1) For U.S. citizens (personnel prescribed in paragraph 2-113 for PCL's and personnel required to be cleared by the government under paragraph 24a, ISM), a NAC is required.

(2) For U.S. citizens (contractor employees other than those listed in paragraph (1) above), the contractor will clear such personnel in accordance with the provisions of paragraph 24b, ISM. Such clearances may be revoked by DISCO in the event the contractor made an administrative error in granting the clearance or there is a bar to such a clearance, unknown to the contractor, which would have precluded its grant.

(3) For immigrant aliens, a BI is required (see d(2) above and paragraph 2-327 for additional requirements).

g. Interim CONFIDENTIAL Personnel Security Clearances.

(1) U.S. citizens (personnel prescribed in paragraph 2-113 for PCL's, personnel who will require access to NATO CONFIDENTIAL information, and personnel required to be cleared by the government under paragraph 24a, ISM) -- the contracting officer of the UA may request DISCO to grant interim CONFIDENTIAL PCL's when it has been determined that performance of the full investigative requirements prior to granting access to CONFIDENTIAL information to an individual will result in crucial delays in precontract negotiations or the award or performance on a contract. A review of the DD Form 48 and a check of the files of the DCII pending completion of the NAC is authorized as a basis for an interim CONFIDENTIAL PCL.

(2) U.S. citizens with prior industrial PCL's -- an interim CONFIDENTIAL PCL may be granted to a U.S. citizen employee who previously had been issued a LOC for a final CONFIDENTIAL, SECRET, or TOP SECRET clearance, when there has been a lapse in employment for more than 12 months but within 25 months since termination of the employment for which the LOC was issued, provided the employee has been subsequently employed in a position requiring access to CONFIDENTIAL information. Before granting an interim CONFIDENTIAL PCL, DISCO shall: (i) obtain the contractor's certificate indicating the date the previous CONFIDENTIAL, SECRET, or TOP SECRET clearance was issued and by whom it was issued; (ii) conduct a satisfactory review of the DD Form 48 and a

check of the files of the DCII; and (iii) initiate a request for a current NAC. Special authorization as to the need for granting an interim CONFIDENTIAL PCL from the UA is not required.

(3) U.S. citizens (contractor employees other than those listed in paragraphs (1) and (2) above) may not be authorized.

(4) Immigrant aliens may not be authorized.

h. Prior Investigations Conducted by DoD Investigative Organizations. In most instances reinvestigation is not required if an individual: (i) has had no break in employment or clearance with a cleared facility which is greater than 12 months, (ii) has had a previous personnel security investigation conducted by an authorized DoD investigative organization which essentially is equivalent in scope to an investigation required by this regulation, and (iii) has not had any substantive adverse information from any source identified to DISCO. There is no time limitation as to the acceptability of such prior investigation, subject to the provisions of paragraph 2-313 or other similar special programs having specified investigative requirements. In instances when the individual has had a break in employment or clearance in excess of 12 months, or there is no previous investigation, an appropriate investigation must be requested. If there is an appropriate prior investigation, but adverse information becomes known, an investigation shall be requested to substantiate or disprove the adverse information.

2-309 Conversion of Clearances for Civilian and Military Personnel of the Department of Defense and Certain Other Governmental Agencies.

a. User Agency and other Executive Branch Clearances. *

(1) PCL's issued by a UA to civilian or military personnel who are U.S. citizens may be converted to industrial PCL's as follows:

(a) top level civilian or military personnel -- 18 months from the time of separation from active federal service;

(b) retired civilian and military personnel of any grade with 19 years or more of federal service -- 18 months from the date of retirement from active federal service;

(c) for other civilian or military personnel separated or retired from active federal service -- 12 months from the time of separation or retirement from active federal service; and

(d) National Guard and Reserve military personnel who actively participate in the Ready Reserve Program are processed for security clearances by the Military Departments in accordance with the procedures for active duty military personnel as referenced in DoD 5200.2-R (reference (rr)). Such security clearances are valid for conversion to industrial PCL's. Clearances granted to such personnel who have transferred to the standby or retired Reserve also may be converted to industrial PCL's within 12 months of a person's being placed in the standby or retired Reserve. *

(2) Top level civilian personnel are defined as presidential appointees, civil service appointees of the super grades (GS-16 and above), and members of industry advisory committees who have been duly appointed by the head of the T.A. Top level military personnel are those of the general and flag officer ranks.

(3) On receipt of a contractor's request for a PCL of a stated level for present or former civilian employees of government, or military personnel on active service or in the Ready Reserve Program (National Guard and Reserve), DISCO shall check with the following, as appropriate, for information as to the present or former security clearance of the individual and its investigative basis. The DISCO shall request to be advised of any information which indicates that continuance of the clearance for access to classified information may not be clearly consistent with the national interest. (A military TOP SECRET clearance based on a NAC plus 15 continuous years of military service or combined military and government service is a valid basis for converting such clearance. However, military TOP SECRET clearances issued prior to February 15, 1962, may be converted to industrial security clearances when based upon a NAC and 10 continuous years of service. In such cases, a BI is not required for conversion purposes. However, upon conversion of the clearance action, DISCO shall initiate immediate action to satisfy the current investigative requirements of DoD 5200.2-R (reference (rr)).

(a) For former top level civilian employees of the federal government and military personnel, check with PSCF.

(b) For former civilian employees of the Office of the Secretary of Defense, the Director for Personnel and Security, Washington Headquarters Services, the Pentagon, Washington, D.C. 20301.

(c) For current and former civilian employees or military personnel of the Departments of the Army and Air Force, including the Army National Guard and Air National Guard, USA Reserve and USAF Reserve, and also for personnel in standby or retired Reserve, the DCII, Defense Investigative Service, Personnel Investigations Center, P.O. Box 1211, Baltimore, MD 21203. Personnel security clearances granted by the Departments of the Army and Air Force are centrally recorded in the DCII.

(d) For current and former military personnel of the Navy, including the USN Reserve, and also for personnel in the standby or retired Reserve, the Commander, Naval Military Personnel Command (Code NMPC (81)/Pers-81), Washington, D.C. 20370.

(e) For current and former military personnel of the U.S. Marine Corps, including the USMC Reserve, and also for personnel in the standby or retired Reserve, the Commandant, Headquarters, U.S. Marine Corp, (Code MMRB-20), Washington, D.C. 20387.

(f) For former civilian employees of the Navy and the Marine Corps, the Security Officer of the activity where the individual had been last employed.

(g) For former civilian employees of the the National Aeronautics and Space Administration, the Director, NASA Security Office, ATTN: NIS, National Aeronautics and Space Administration, Washington, D.C. 20546. (DISCO will identify the Field Center involved.)

(h) For former civilian employees of GSA, the Director, Office of Internal Security, General Services Administration, Washington, D.C. 20405.

(i) For former civilian employees of Department of State, the Chief, Division of Domestic Operations, Office of Security, Department of State, Washington, D.C. 20520.

(j) For former civilian employees of Department of Commerce, the Director, Office of Security, Department of Commerce, Washington, D.C. 20230.

(k) For former civilian employees of the Small Business Administration, the Security Officer, Office of the Inspector General, Small Business Administration, Washington, D.C. 20416.

(l) For former civilian employees of the National Science Foundation, the Security Officer, Office of Personnel, National Science Foundation, Washington, D.C. 20550.

(m) For former civilian employees of the Department of Treasury, The Assistant Director of Personnel (Personnel Security), Treasury Department, Washington, D.C. 20020. *
*
*

(n) For former military personnel of the Coast Guard, the Chief, Intelligence and Security Division, Office of Operations, U.S. Coast Guard, Washington, D.C. 20593.

(o) For former civilian employees of the U.S. Coast Guard, the Chief, Personnel Security Branch, Personnel Service Division, U.S. Coast Guard, Washington, D.C. 20593.

(p) For former civilian employees of the Department of Transportation, the Director, Office of Security, Department of Transportation, Washington, D.C. 20590.

(q) For former civilian employees of the Department of Agriculture, the Chief, Security, Employee Management and Training Staff, Office of Personnel, Department of Agriculture, Administration Building, Washington, D.C. 20250.

(r) For former civilian employees of FEMA, the Director, Office of Security, Federal Emergency Management Agency, Washington, D.C. 20472.

(s) For former civilian employees of the Department of the Interior, the Chief, Enforcement and Security Management Division, Office of Administrative Services, Department of the Interior, Washington, D.C. 20240.

(t) For former civilian employees of the Department of Labor, the Director, Personnel Management, Office of the Assistant Secretary for Administration and Management, Department of Labor, Washington, D.C. 20210.

(u) For former civilian employees of EPA, The Assistant Inspector General, Office of Management and Technical Assessment, Environmental Protection Agency, Washington, D.C. 20460.

(v) For former civilian employees of the Federal Reserve System, the Chief of Security, Division of Support Services, Board of Governors, Federal Reserve System, Washington, D.C. 20551.

(w) For former civilian employees of the Department of Justice, the Director, Security Staff, Department of Justice, Washington, D.C. 20530.

(x) For former civilian employees of the U.S. Arms Control and Disarmament Agency, the Security Officer, U.S. Arms Control and Disarmament Agency, Washington, D.C. 20451.

(y) For former civilian employees of the White House Office staff and those persons cleared by the White House, the White House, ATTN: Security Office, Washington, D.C. 20500.

(z) For former civilian employees of the GAO, the Director, Office of Security and Safety, U.S. General Accounting Office, Washington, D.C. 20548.

(aa) For former employees of the USIA, the Director, Office of Security, United States Information Agency, Washington, D.C. 20547.

(4) Following the verification of previous PCL, a LOC for the appropriate level shall be issued by DISCO to the facility, provided:

(a) the investigative basis meets the current requirements of DoD 5200.2-R (reference (rr)), and

(b) the former clearing authority reports there is no information indicating that continuance of the clearance is not clearly consistent with the national interest.

(5) Applications for conversion of clearance are made by submission of DD Form 48-3. In addition, except in the case of individuals currently employed by the federal government or on active military duty, the application shall include an exact reproduction of Standard Form 50, "Notification of Personnel Action," in the case of former civilian employees of the government, or DD Form 214, "Certificate of Release or Discharge from Active Duty," in the case of former military personnel. However, the individual being considered for a PCL shall be required to accomplish all forms required by this regulation for an individual with no previous clearance when:

(a) the basis of the investigation does not meet the *
current requirements of DoD 5200.2-R (reference (rr)); *

(b) the clearance requirement is for a higher level than
is reflected in the clearance records;

(c) there has been a greater lapse of time than that set
forth in paragraph a above;

(d) there is information which indicates that granting of
a clearance may not be clearly consistent with the national interest; or

(e) the DISCO is unable to verify the prior clearance,
determine the investigative basis thereof, or obtain an answer to the question
as to whether continuation of the clearance may be clearly consistent with the
national interest.

b. Department of Energy (DOE) and Nuclear Regulatory Commission (NRC) Clearances. The "Q" and "L" clearances granted by DOE and NRC are considered acceptable for issuance of a DoD industrial PCL. The "Q" clearance is considered an authoritative basis for a DoD clearance at the TOP SECRET level and the "L" clearance is considered an authoritative basis for a DoD clearance, at the SECRET level. A contractor may request a DoD industrial PCL for an employee who currently has a "Q" or "L" PCL or previously held such a clearance, when there has not been a lapse of more than 12 months since termination of the PCL. Application for a DoD industrial PCL based on a "Q" or "L" clearance may be made by submitting one copy of the DD Form 48-3 to DISCO. The "Job Title and Description of Duties" block in part 1 of the DD Form 48-3 will be annotated: "DOE (or NRC) 'Q' (or 'L') Conversion Requested." The "Q" or "L" number, if known, will be indicated. Prior to issuing a LOC to the contractor, DISCO will obtain verification of the "Q" or "L" clearance, the date the investigation was completed, the name of the investigative agency and case file number, if available, and a statement from DOE or NRC that no derogatory information has developed since the clearance was granted which has not been resolved. DISCO can obtain the required information by writing to: (i) Director, Safeguards and Security, U.S. Department of Energy, Washington, D.C. 20545, or (ii) Director, Division of Security, U.S. Nuclear Regulatory Commission, Washington, D.C. 20555.

c. The contractor will be advised that the individual being
considered for a PCL must accomplish all forms required by this regulation for
an individual with no previous clearance when:

(1) the existence of "Q" or "L" clearance cannot be verified,

(2) there has been a lapse of more than 12 months since
termination of the clearance, or

(3) the required statement that no unresolved or derogatory
information has developed since the clearance was issued is not received from
DOE or NRC. (If a statement is received that unresolved or derogatory
information has been developed, it will also be necessary to request the
contractor to have the employee complete all forms necessary for an initial
clearance request.)

d. Investigations Conducted and Clearance Granted by Other Agencies of the Federal Government. Whenever a prior investigation or personnel security determination (including clearance for access to information classified under Executive Order 12356 (reference (w)) of another agency of the Federal Government meets the investigative scope and standards of DoD 5200.2-R (reference (rr)), such investigation or clearance may be accepted for the investigative or clearance purposes of the Regulation, provided that the employment with the Federal agency concerned has been continuous and there has been no break longer than 12 months since completion of the prior investigation, and further provided that inquiry with the agency discloses no reason why the clearance should not be accepted. If it is determined that the prior investigation does not meet the provisions of this paragraph, supplemental investigation shall be requested. The procedures provided in paragraphs a(4) and (5) above apply. *

2-310 Administrative Termination of Personnel Security Clearances.

a. Requests for administrative termination of PCL's submitted to DISCO in accordance with paragraph 29a, ISM, shall be reviewed for accuracy and completeness. If the "Personnel Security Clearance Change Notification" (DISCO

Form 562) has been signed by the contractor and the employee, DISCO will reflect the change in the PSCF and the date the administrative termination action was completed. The DISCO will advise the contractor by automated letter of the completed action. Contractor-granted CONFIDENTIAL clearances which are administratively terminated will be handled in accordance with the requirements outlined in paragraph 29, ISM.

b. When the DUSD(P), ATTN: DSP&P, or higher authority, determines that a PCL or PCL action in process was requested or granted in error or is no longer required, he or she may, at his or her option, direct an administrative termination of such clearance or clearance action in process without prejudice to the individual concerned or jeopardy to the individual's employer's operations. The DISCO shall advise the CSO, the contractor, and the individual concerned, as appropriate, that:

(1) the PCL or PCL action in process is being administratively terminated because it was initiated or issued in error or is no longer required;

(2) the action in no way reflects adversely on the individual or his or her personnel security eligibility; and

(3) the provisions of this paragraph shall not operate to conflict with paragraph 2-308f(2).

The DISCO records shall be annotated to reflect the action taken. PCL's or PCL actions so terminated may be revalidated in accordance with procedures established in paragraph 29, ISM.

c. If the request submitted to the CSO pertains to an OODEP, it will be reviewed to ensure that the request is justified and the individual is an OODEP who is excludable. If the request is proper, DISCO Form 562 will be annotated to reflect that the CSO concurs in the recommendation and then be forwarded to DISCO with one copy of the organization's minutes required by paragraph 22e(1), ISM. The CSO will also amend the FCL records, as appropriate, prior to forwarding the DISCO Form 562 to DISCO. The DISCO will:

(1) change the PSCF to reflect the date of the requested action, and

(2) advise the contractor by automated letter of the completed action.

d. If a case is referred to the CSO in accordance with paragraph 29e, ISM, the employee will be requested (certified mail, return receipt requested) to show cause within 30 days as to why the recommended action should not be completed. If the individual fails to respond within 30 days from receipt of such request to show cause, the failure to respond will be considered a valid indication that the employee no longer objects to the administrative termination of his or her clearance and the case shall be referred to DISCO for appropriate action. If the individual presents justification for retention of clearance, which in the judgment of the CSO is adequate, the contractor and the employee shall be advised that the request for administrative termination is not approved and the clearance shall remain in effect. If, in the judgment of the CSO, the employee has not submitted

adequate justification, the case, with appropriate rationale and recommendations will be referred to the Director, DIS, ATTN: Deputy Director (Industrial Security) for final determination. The Director, DIS, ATTN: Deputy Director (Industrial Security) will notify DISCO, the CSO, the contractor, and the employee of the final decision in the matter. The Director, DIS will make the final determination in administrative termination of PCL cases in which the employee has objected to termination action.

2-311 Administrative Downgrading of TOP SECRET Personnel Security Clearances.

a. Requests for administrative downgrading of TOP SECRET PCL's submitted by contractors pursuant to paragraph 30, ISM, shall be reviewed by DISCO for completeness and accuracy. If the DISCO Form 562 is complete and signed by the contractor's FSO, the DISCO will make the necessary change to the PSCF and will advise the contractor by automated letter of the downgrading action.

b. The DISCO will reinstate TOP SECRET PCL's which have been downgraded to a lower level, provided a requirement for such access exists and there has not been a lapse of more than 24 months from the date of the downgrading action. On receipt of a properly completed and signed DISCO Form 562 requesting a reinstatement of clearance, the DISCO will make the required change in the PSCF and advise the contractor of the date of the reinstatement by issuance of a new LOC for TOP SECRET. The new LOC will bear the date of the upgrading action.

c. When there has been a lapse of more than 24 months from the date of the downgrading action, DISCO will issue a new LOC, provided the individual has been continuously employed by the same contractor since the date of the downgrading action and a valid need exists for the TOP SECRET clearance. If the contractor knows of no questionable or adverse information, the contractor shall make application for the new LOC by submitting one copy of DD Form 48-3 to DISCO. If the DISCO review of the DD Form 48-3 and other sources confirms that there is no adverse information present and the individual has had a BI conducted at any time during his or her employment with this contractor, a new LOC will be forwarded to the contractor. In the event the case involves adverse information, an investigation will be requested to substantiate or disprove the adverse information.

2-312 RESTRICTED DATA, Additional Clearance Requirements.

a. When access to CONFIDENTIAL RESTRICTED DATA as defined in the Atomic Energy Act of 1954 (reference (c)), as amended, is required by any contractor employee, other than one who has been cleared by the DoD based on a NAC under the provisions of paragraph 24a, ISM, DISCO will obtain a NAC.

b. Requirements for clearances for access to TOP SECRET or SECRET RESTRICTED DATA shall be in conformance with paragraphs 2-308b, c, or d, as applicable.

c. Interim SECRET, interim CONFIDENTIAL, or contractor CONFIDENTIAL PCL's do not meet this requirement and their use for access to RESTRICTED DATA information is not authorized. Interim TOP SECRET PCL's are valid for access to RESTRICTED DATA no higher than SECRET.

2-312.1 Requirements for Access to CNWDI. A final TOP SECRET or SECRET PCL granted in accordance with paragraph 2-312a, b, or c above, is valid for access to CNWDI of the same or lesser security classification, provided the individual has been given a CNWDI security briefing. In rare instances an immigrant alien may possess a unique or very unusual talent or skill that is essential to the U.S. Government and not possessed to a comparable degree by an available U.S. citizen. In such exceptional cases, an affirmative decision shall be made that it is in the overall best interests of the U.S. to grant CNWDI access to an immigrant alien. In such cases the contractor must submit a request to the contracting officer with full justification. If the contracting officer determines that the justification is appropriate in accordance with the foregoing criteria, the case will be forwarded through appropriate channels via the head of the UA to the DUSD(P), ATTN: DSP&P.

2-313 Requirements for Access to Classified COMSEC Information.

a. Access to classified COMSEC information may be afforded U.S. citizens who have been granted a final PCL by the U.S. Government and have a need-to-know. An interim TOP SECRET clearance is valid for access to COMSEC information; however, only at the SECRET level and below. Contractor employees who are immigrant aliens are not eligible for access to classified COMSEC information.

b. Before a COMSEC account can be established and a contractor may receive or possess COMSEC material accountable to a COR, individuals occupying the positions of FSO, COMSEC custodian, and alternate COMSEC custodian must possess a PCL based on a BI current within 5 years and have been given a COMSEC briefing (see paragraph d below) 11/. The BI relative to a "Q" clearance is acceptable provided it is current as required.

c. On receipt of a request from a contractor (see paragraph 15b, CSISM) for the basis of the current PCL granted to the FSO, the COMSEC custodian, and alternate COMSEC custodian DISCO shall accomplish the following.

(1) Review the PSCF to ascertain the investigative basis and the date the most recent periodic reinvestigation was completed.

(2) Provide the contractor, with a copy to the contractor's CSO, the basis for the current PCL and the date of the BI, and, if appropriate, the date of the latest periodic reinvestigation.

(3) If an individual occupying any of the three positions identified above has not been the subject of a BI current within 5 years, request the contractor to submit a completed DD Form 49 and FD Form 258.

11/ Until the required BI's are favorably completed, a COMSEC account may be established to receive and hold SECRET COMSEC material. No material designated CRYPTO shall be released to the account until completion of the BI's.

(4) On receipt of the DD Form 49 and FD Form 258, initiate action to obtain a current BI.

(5) If the BI is favorable, annotate the individual's PSCF and forward notification to the contractor with a copy of the notification to the contractor's CSO.

d. The DISCO shall be responsible for initiating action to provide for the required update of the BI by requesting the contractor whose employee(s) are involved to process new clearance forms 6 months prior to the 5-year anniversary date of the previous BI.

e. A representative of the U.S. Government shall brief the FSO, the COMSEC custodian, and the alternate custodian. If the briefing is not conducted by the CSO, the government representative that conducted the briefing shall provide the CSO written notification upon completion of the briefing. Other contractor employees will be briefed by the FSO, the COMSEC custodian, alternate COMSEC custodian, or another appropriate individual designated in writing by the FSO prior to being authorized access to classified COMSEC information. (For contractor activities on a UA installation, the provisions of paragraph 1-108, ISR, apply.)

2-314 COMSEC Briefing and Debriefing Requirements.

a. All contractor personnel who require access to classified COMSEC information in the performance of their duties shall be briefed before access is granted. The FSO, the COMSEC custodian, and the alternate custodian will be briefed by government representatives as set forth in paragraph 2-313. Other contractor personnel will be briefed by the contractor. The purpose of the briefing is to ensure that the employee understands:

(1) the unique nature of COMSEC information and its unusual sensitivity,

(2) the special security requirements for the handling and protection of COMSEC information, and

(3) the penalties prescribed in Title 18, U.S.C., §§ 793, 794, and 798 (reference (nn)), for willful disclosure of COMSEC information.

b. All personnel having access to COMSEC information shall be given a periodic rebriefing at least annually. The rebriefing will be conducted by those individuals designated in paragraph a above to give the initial briefings. These briefings shall emphasize particularly any security deficiencies noted during recurring inspections.

c. The FSO, COMSEC custodian, and alternate custodian shall be given an oral debriefing by a representative of the U.S. Government within 90 days after the need for access to COMSEC information is discontinued. If one of these individuals remains employed, the contractor shall submit a report to DISCO providing the person's name and social security number and advising that the individual no longer requires a BI, current within 5

years, for access to COMSEC information. Other employees shall be given an oral debriefing by the contractor. The contractor shall maintain a record of all debriefings for a minimum of 3 years.

2-315 Additional Requirements for SENSITIVE COMPARTMENTED INFORMATION Material.

a. The provisions of the LSM apply to research, development, and production of SENSITIVE COMPARTMENTED INFORMATION. In addition, special security requirements supplementing the LSM may be prescribed by a UA for SENSITIVE COMPARTMENTED INFORMATION contracts. For SENSITIVE COMPARTMENTED INFORMATION contracts awarded by military department procurement activities on behalf of the NSA, the NSA will prescribe the special security requirements.

b. In the case of SENSITIVE COMPARTMENTED INFORMATION contracts awarded by military department procurement activities for NSA, NSA shall be responsible for exercising security controls over the contract.

c. When access to NSA SENSITIVE COMPARTMENTED INFORMATION material or information is involved, special procedures for processing clearances shall be as prescribed by NSA.

d. Personnel access authorizations for SENSITIVE COMPARTMENTED INFORMATION shall be processed in accordance with paragraph 1-305d.

e. In the case of SENSITIVE COMPARTMENTED INFORMATION contracts awarded by and for a UA, an activity designated by the UA, shall be responsible for exercising security controls over the contract.

f. Access to SENSITIVE COMPARTMENTED INFORMATION will be granted to contractor employees requiring access by the activity designated to exercise security controls over the contract as provided above.

g. Denial or revocation of authorization for access to SENSITIVE COMPARTMENTED INFORMATION is not appealable.

2-316 Denial of Admittance to User Agency Installations.

a. The provisions of this regulation shall not be interpreted as modifying in any way the authority of the Commander or Head of a UA installation to deny admittance of any individual to an installation under his or her control.

b. A PCL under the DoD Industrial Security Program shall not be requested for the purpose of determining an individual's eligibility for admittance to a UA installation when access to classified information is not involved.

c. Denials of admittance to a UA installation are not appealable under the DoD Industrial Personnel Security Clearance Program.

2-317 Intelligence Briefing and Debriefing Requirements. The UA activity controlling the contract and the activity to be visited by contractor employees are responsible for complying with the applicable policy covering the release

of intelligence information to contractors and for advising contractors and their employees of restrictions pertaining to the reproduction, release, dissemination, or disposition of intelligence information given to the contractors or their employees. Briefing and debriefing requirements in addition to those imposed by paragraph 5g, ISM, shall be provided by, or in accordance with, instructions of the UA 12/.

2-318 CONFIDENTIAL Security Clearances for Personnel of Colleges and Universities. Before granting access to CONFIDENTIAL information to U.S. citizens employed by colleges and universities, the completion of a NAC with favorable results is required. The provisions of this paragraph are not retroactive. PCL's previously granted under the old procedures remain valid as long as the individuals continue to be employed by the same college or university. However, clearances granted under the old procedures are not transferable.

2-319 Types of Personnel Investigations. The types of personnel security investigations required for the various personnel security clearance actions are outlined in DoD 5200.2-R (reference (rr)). No other types of investigations are authorized.

a. NAC for Personnel. A check of specific national agencies for information concerning the person who is subject to investigation. In the event derogatory or questionable information concerning the individual is disclosed by a NAC or by the applicant, the inquiry will be extended as necessary to obtain such additional information as may be required to substantiate or disprove the information. The DISCO shall specifically direct attention to derogatory information disclosed by the applicant in the PSQ to the Personnel Investigations Center (PIC) for appropriate use and transmittal to the designated investigative elements when requesting a NAC.

b. Background Investigation. A BI is a thorough and complete investigation to develop information as to whether the access to classified information by the individual being investigated is clearly consistent with the national interest. It shall make inquiry into pertinent facts bearing on the individual's trustworthiness, integrity, reputation, and loyalty to the U.S. A BI shall be conducted in accordance with the DoD standards on this subject. It shall normally cover the 5-year period (15 years for an immigrant alien) of the individual's life immediately preceding the investigation or from the date of the individual's eighteenth birthday whichever is the shorter period (but at least 5 years in the case of immigrant aliens regardless of age), unless:

(1) derogatory information is developed in the course of the investigation, in which event the investigation shall be extended to any period of the individual's life necessary to substantiate or disprove the information, or

12/ The policy on the release of intelligence information is contained in Director of Central Intelligence Directive No. 1/7 (reference (oo)). The directive is implemented within DoD by DoD Instruction 5230.22. Release to contractors is defined in the directive as the visual, oral, or physical disclosure of classified information.

(2) additional investigation is specifically required by competent authority (for example, DISCO, DISCR, and Director, DIS).

c. Other Investigations. Whenever a prior investigation by any investigative agency of the federal government meets the standards prescribed by the DoD, eligibility for clearance may be determined under the conversion procedures of paragraph 2-309 based on the review of the prior investigation, provided that service by the employee, in a cleared status, has been continuous since that investigation with no break in service longer than 12 months. Such acceptance shall be conditioned upon an inquiry by DISCO to the previous employer(s) which discloses no reason why the investigation should be expanded or updated, with the possible resulting requirement for adjudication under the DoD Industrial Personnel Security Clearance Program.

2-319.1 User Agency Responsibility to Report Adverse Information. The Commander or Head of a UA activity shall report to DISCO any adverse or questionable information which comes to his or her attention, concerning a contractor employee who has been cleared, or is in the process of being cleared, for access to classified information, which may indicate that such access is not clearly consistent with the national interest.

2-320 Denial, Suspension, or Revocation of Personnel Security Clearances.

a. In the event adverse information is developed by a review of records or investigation, the scope of the inquiry will be enlarged to the extent necessary to obtain such additional information as may be required as a basis to determine whether or not a PCL may be granted. The DISCO may not deny a PCL to a contractor's employee, but shall make a recommendation to deny such PCL when information disclosed by an investigation indicates that the granting or continuance of a PCL is not clearly consistent with the national interest. This recommendation, with a report of all pertinent facts, shall be transmitted promptly to the DISCR, OGC, OSD. A copy of the recommendation shall be transmitted promptly to HQ DIS.

b. In the event adverse information is obtained concerning an individual who previously had been granted a clearance by the government or by a contractor, an inquiry shall be initiated to obtain such additional information as may be required as a basis to determine whether or not the clearance should be revoked. When the information developed indicates that revocation appears justified, DISCO shall address recommendations to the DISCR, OGC, OSD. A copy of the recommendations shall be transmitted promptly to HQ DIS.

c. Whenever there is probable cause to believe, on the basis of all the facts available, that interim action is warranted in the interests of national security, the PCL shall be temporarily suspended pending a final determination by DISCR, OGC, OSD. DISCO or the CSO shall recommend suspension action to the Director, DIS, Attn: Deputy Director (Industrial Security). These cases will be afforded the highest possible priority and acted on expeditiously. Suspension under this regulation shall be taken only by the Director, DIS or, when absent, by the Deputy Director (Industrial Security), HQ DIS after coordination with the OGC, OSD, and the ODUSD(P). The authority to invoke suspension action may not be further delegated. On taking the suspension action, DIS shall immediately notify: (i) the individual concerned and provide reasons for the action, (ii) the facility to which the LOC for the

individual was granted, (iii) the CSO, (iv) DISCO, and (v) all concerned UA and procurement activities. The CSO shall request the facility to provide positive assurance that the individual will not have, and can be effectively excluded from, access to all classified information in the possession of the facility, and that all outstanding visit authorizations requiring access by the individual have been canceled. The facility is to be placed on notice that the suspension of clearance is a temporary action pending a final determination by DISCR. In all cases where the suspension action involves an OODEP, the eligibility of the FCL shall be reviewed. The CSO shall apply the procedures as appropriate under paragraph 2-12ld, the same as if DISCR had taken the suspension action. The Director, DIS shall give top priority in completing the investigation of the case. A full report of the case shall be made promptly to the DISCR, OGC, OSD.

d. The withdrawal of an interim PCL as described in paragraph 2-301b, ISR, shall not be construed as denial, suspension, or revocation of clearance and referral of the case to the DISCR, OGC, OSD, is not required prior to the completion of the investigation; however, the DISCR, OGC, OSD, shall be notified promptly of all such withdrawals of interim PCL and the basis for it.

e. In the event a determination has been made by DISCR to authorize access to CONFIDENTIAL or SECRET information and a subsequent requirement develops for access to a higher classification level than was authorized by DISCR, DISCO shall request that the investigation be brought up to date and shall submit the case together with a recommendation and a report of all pertinent facts of the DISCR, OGC, OSD for a determination with respect to the higher level of access requested.

f. In the event a determination is made under the procedure established in DoD 5220.6 (reference (11)) that an individual is eligible for a PCL, such clearance shall be granted by DISCO only if the requirement for it still exists. When the PCL is not granted, the contractor and the employee concerned shall be advised of the individual's security eligibility for a PCL and that such clearance can be revalidated in accordance with paragraph 29, ISM.

g. Information developed in the course of official investigations may be disclosed only to those who have an official requirement for such information. DoD policy strictly prohibits the disclosure of information developed by official investigation to a contractor who is the employer of the subject of the investigation. Therefore, to ensure continuing compliance with this fundamental requirement, the following guidance is provided.

(1) No unfavorable information on an individual being considered for an access authorization shall be discussed or transmitted in any manner to a representative of a company where such an individual is employed.

(2) Any interrogation of, or discussions with, employees or other persons during the course of an official inquiry or investigation of an employee shall be conducted in such a manner as to avoid conveying to the person interviewed, to the maximum extent possible, the derogatory information that may have come to the attention of the DoD.

(3) Particular care shall be exercised to avoid communicating, either formally or informally outside official government channels, substantive information of a derogatory nature pertaining to an individual who has received a final favorable determination.

2-321 Access to NATO Classified Information. A final PCL granted by the DoD for U.S. citizens is valid for NATO information of the same or lesser security classification, provided the individual has been given a security briefing in accordance with paragraph 85d, ISM. If access to COSMIC/TOP SECRET is involved, the individual shall sign a certificate to the effect that he or she has been briefed on his or her responsibilities for safeguarding COSMIC/TOP SECRET information. CONFIDENTIAL clearances granted by the contractor are valid for access to NATO RESTRICTED information only. Interim CONFIDENTIAL or interim SECRET clearances granted by DISCO are not valid for access to COSMIC/TOP SECRET, NATO SECRET, or NATO CONFIDENTIAL information. An interim TOP SECRET PCL is valid for access to NATO information classified no higher than SECRET. Immigrant aliens or aliens issued reciprocal clearances are not authorized access to NATO classified information (see paragraphs 20c, 24a(2), 31c, 85d, and 86, ISM).

2-322 U.S. Security Assurances for U.S. Citizens Under Bilateral Reciprocal Security Agreements. When a foreign government with whom the DoD has entered into a bilateral reciprocal industrial security agreement (pursuant to paragraph 2-117) desires that a U.S. citizen be cleared for access to that government's information, DIS will follow the procedures established by the applicable agreement.

2-323 Security Assurances for Nationals of Signatory Governments Under Bilateral Reciprocal Industrial Security Agreements. When a national of a foreign government which has entered into a bilateral reciprocal industrial security agreement with the DoD (paragraph 2-117) requires a PCL for access to U.S. classified information, DIS will follow the procedures established by the applicable agreement. Persons granted reciprocal clearances under the provisions of this agreement are subject to the access limitations set forth in paragraph 2-117a(1) through (7).

2-324 Requirements of the Nuclear Weapon Personnel Reliability Program (PRP).

a. Contractor employees assigned to training for, or performance of, duties in critical or controlled positions as defined in DoD Directive 5210.41 (reference (pp)) shall be screened, evaluated, and certified by the certifying official in accordance with requirements and procedures set forth in DoD Directive 5210.42 (reference (qq)).

b. Contractor employees who are found not qualified under the PRP shall be so advised in writing of the reasons for their disqualification and of their rights to request reviews by the reviewing official on an individual basis.

c. Certifying officials and reviewing officials, as defined in reference (qq), shall be designated formally in writing.

d. Contracting officers shall include in contracts which involve the Nuclear Weapon PRP the requirements and responsibilities of the contractor as set forth in enclosure 2 of reference (qq).

2-325 Reserved.

2-326 Reserved.

2-327 Immigrant Alien Clearance for Access to SECRET and CONFIDENTIAL Information. On receipt of a contractor's request for authority to process an immigrant alien for a SECRET or CONFIDENTIAL clearance, the contracting officer shall forward the request to the appropriate official ^{13/} designated in appendix F, DoD 5200.2-R (reference (rr)). On receipt of the approval or denial of the authorization request by the designated official, the contracting officer shall so forward the decision to the requesting contractor and provide an information copy to DISCO (or to the CSO if the immigrant alien is an OODEP). Clearances granted to immigrant aliens are not transferable except in the case of a MFO and will be administratively terminated on termination of employment.

Part 4. MAINTENANCE OF FACILITY FILES AND DISCO RECORDS

2-400 Application.

a. Each CSO will be responsible as the official and sole office of record for the maintenance of all documents and records pertaining to contractor facilities under cognizance.

b. The DISCO shall maintain clearance records pertaining to contractor FCL and PCL actions.

2-401 Maintenance of Facility Folders. The file folder on each facility shall contain all original documentation with respect to the facility to include, but not limited to, the following:

a. initial request for FCL and justification for retention or continuation;

b. the DD Form 441 with DD Form 441-1, when applicable -- the CSO of each facility of a MFO shall forward the original DD Form 441-1 to the CSO of the HOF;

c. the DD Form 441s and all correspondence and associated documentation, including agreements and determinations pertaining to FOCI factors in the case;

d. data required on HOF or parent, if and when applicable;

^{13/} Non-DoD UA's should submit their requests to the Head of the UA or the appropriate designee.

e. actions by boards of directors or similar executive bodies, as prescribed by paragraph 2-113;

f. the DD Form 374;

g. DIS FL 381-R and all relevant correspondence pertaining thereto;

h. the DIS Forms 1149 and 1150, when used;

i. the DIS Form 1148, when used; and

j. all relevant documentation, whenever the FCL has been denied, suspended, or revoked for cause in accordance with paragraph 2-113 of this regulation.

2-402 Responsibilities of the Cognizant Security Office.

a. In addition to maintaining the file folder with contents as described in paragraph 2-401 above, the CSO shall be responsible for ensuring that the very latest security inspection results are available in order to promptly provide UA's and other requesters information in connection with the current clearance status and ability to physically safeguard classified material.

b. CSO's shall be responsible for promptly forwarding a legible copy of DIS Form 553 to DISCO under the following circumstances:

(1) when initiating a FCL;

(2) when granting an interim FCL;

(3) on granting a completed FCL;

(4) when there is a significant change in the facts pertaining to a facility such as a change of name, address, ownership, or level of the FCL;

(5) on invalidating a FCL;

(6) when processing an invalid FCL to a valid status; and

(7) on downgrading or termination of a FCL under paragraphs 2-111 or 2-119, or on suspension or revocation of a FCL under paragraph 2-121.

c. When a FCL action is reported to DISCO, the interim, pending, or completed nature of the action shall be clearly indicated. When a DIS Form 553 supersedes one previously submitted to DISCO, this shall be clearly indicated on the new card.

d. CSO's shall be responsible for promptly forwarding to DISCO any information received from a contractor concerning:

(1) termination of an employee, indicating the reason for termination;

(2) the elevation of a cleared employee to the position of an OODEP, or the deletion of a cleared individual from a position of an OODEP when the PCL is to be retained at the current level; or

(3) refusal of a terminated employee to sign the security termination statement as prescribed by paragraph 5g, ISM, provided the inquiry required by paragraph 5-106 indicates that the refusal was deliberate. The CSO shall report the reason for termination of employment, the circumstances surrounding the individual's refusal to sign the termination statement, and the identification of the activity where the report of the incident is filed. If the failure to sign the termination statement was due to an omission during the termination proceedings as contrasted with a refusal to do so, this fact shall be clearly indicated on the report submitted to DISCO.

2-403 Responsibilities of DISCO.

a. When contractor personnel are cleared for access to classified information by DISCO, such information will be made a matter of record in the PSCF. DISCO will verify PCL status only to cleared DoD contractors, UA's, and other authorized government agencies.

b. On notification of the death or termination of employment of such cleared contractor personnel, DISCO shall make such information a matter of record in the file.

c. DISCO shall also annotate its records and maintain the file to reflect any change in the clearance status of the contractor employee, including such actions as suspensions and revocations.

d. On receipt of the DIS Form 553 from the CSO, DISCO shall enter such information into its record system. DISCO shall update its records, as appropriate, on receipt of any subsequent DIS Forms 553 submitted by the CSO on the facility.

2-404 Use of Information.

a. Authorized requesters may obtain verification of PCL's on contractor personnel by submitting requests for such information to DISCO which adequately identifies the individual as follows: the individual's last name, first name, middle name, date and place of birth, and social security number if known. The DD Form 555 may continue to be used for this purpose.

b. Requests for information pertaining to contractor facilities are to be submitted to the appropriate CSO.

SECTION III. VISITORSPart 1. VISITS TO USER AGENCY CONTRACTORS

3-100 Application. This part establishes procedures and responsibilities to be exercised by UA's and CSO's for visits to contractors of UA's where access to classified information is involved. The procedures to be followed by contractors are detailed in section V, ISM.

3-101 General.

a. The general policies and procedures applicable to visits to UA contractors are contained in paragraph 37, ISM. Industrial security representatives of the DoD and other UA's and representatives of U.S. Government investigative agencies and the DUSD(P), are not considered as visitors under this section when acting in their official capacities as set forth in paragraph 37h, ISM.

b. The number of visitors requiring access to classified information shall be held to a minimum and the following requirements must be established:

(1) that the visit is necessary, and

(2) the purpose of the visit cannot be achieved without access to classified information.

c. Approval of the visit normally constitutes the authority for the disclosure of classified information. In the event the visit is disapproved, the requester shall be promptly notified by the contractor or activity which made such decision (see paragraph 37c, ISM). Approval in addition to that of the contractor being visited is required as follows:

(1) Category 1 visits -- none (see paragraph 3-103a),

(2) Category 2 visits -- contracting officer of the requesting contractor (see paragraph 3-103b),

(3) Category 3 visits -- contracting officer of the UA whose information is involved (see paragraph 3-103c),

(4) Category 4 visits -- UA (see paragraph 3-103d), and

(5) Category 5 visits -- CSO of contractor being visited and DISCO (see paragraph 3-103e).

d. Request for visits shall be submitted to the contractor or activity being visited in writing (mail or teletype) in advance of the proposed visit. In exceptional cases the telephone may be used provided the visit is confirmed in writing. Under no circumstances, however, may employees hand-carry their own visit requests to the place being visited. All visit requests shall contain the information required by paragraph 37d, ISM, except as otherwise stated.

e. Visit requests which involve access to information requiring special access authorizations (for example, CRYPTO information, NATO, or other special or limited access programs) will, in addition to the information required by paragraph 37d, ISM, include the information required by paragraph 37e, ISM.

3-102 Long-Term Visits. Long-term visits of employees of one contractor temporarily stationed at a facility of another contractor are handled in accordance with paragraph 40, ISM. The CSO, however, is responsible for conducting periodic inspections to ensure that classified information in possession of the visiting employees is properly safeguarded, and for notifying the host contractor of any security deficiencies found during the CSO's regularly scheduled inspections at the host facility.

3-103 Visitor Categories and Procedures. Categories and procedures applicable to visits of UA contractors are provided in paragraph 41, ISM. Specific responsibilities of government agencies (other than those specified in paragraph 3-101b), their contracting officers, or the CSO are as follows.

a. Category 1. This category includes visits where a contractual or prospective contractual relationship exists between contractors or between a contractor and a UA, and visits to a contractor by: representatives of the Government Accounting Office (GAO) for auditing purposes, authorized representatives of the Department of Labor, and other agencies of the executive branch of the government, when acting in their official capacities (see paragraph 41a, ISM).

(1) Such requests will be forwarded to the contractor to be visited.

(2) Representatives of DoD UA's are reminded to comply with paragraph 20-802 of the DAR (reference (c)) prior to forwarding visit requests to the contractor.

b. Category 2. This category applies to visits between contractors who have been granted FCL's where a contractual relationship does not exist and which do not otherwise meet the requirements of Category 1. The requesting contractor shall obtain verification of the visitor's need-to-know from his or her contracting officer (see paragraph 41b, ISM, and paragraph 3-101c (2) above). Approval of the visit by the contracting officer will be in writing and included as part of or attached to the visit request. The contracting officer will certify to the visitor's need-to-know only after it has been clearly established that the visit and proposed release or acquisition of classified information at the facility to be visited is necessary in the furtherance of a UA contract (see paragraph 41b, ISM).

c. Category 3. This category applies to representatives and employees of the DOE and its contractors whose visits to the facility of a UA contractor will require access to other than RESTRICTED DATA (see paragraph 41c, ISM).

(1) The activity requesting the visit will furnish the required information "Request for Visit or Access Approval" (DOE Form F 5631.20) concerning the proposed visit to the contracting officer of the contractor

whose classified information is involved. Through direct coordination with the activity requesting the visit, the contracting officer shall determine that there is sufficient justification for the visit; that is, that the visit will further the performance of current or future UA or DOE contracts.

(2) The contracting officer shall, if the visit is approved, notify the contractor of the visit approval, including required information concerning the visitor (DOE Form F 5631.20).

d. Category 4. Except as authorized in subparagraph 3-103d(8) *
below, visits to contractor facilities by foreign nationals (see paragraph *
1-232) and persons acting as representatives of a foreign interest (see *
paragraph 1-256), hereafter referred to collectively as foreign represen- *
tatives, must be officially sponsored by a foreign government. Foreign *
sponsorship is normally reflected in an official request for a visit from *
the embassy of the nation concerned to the cognizant UA foreign disclosure *
office 1/. The cognizant UA may then sponsor, deny, or elect not to sponsor *
the visit. UA sponsored visits shall not be used to avoid the licensing *
requirements of the ITAR published by the Department of State or the Export *
Administration Regulations published by the Department of Commerce. The *
contractor shall be responsible for ensuring that both sponsored and un- *
sponsored visits by foreign representatives are effectively denied *
unauthorized access to: (i) classified information, (ii) unclassified *
technical data governed by the Export Administration Act, administered by *
the Secretary of Commerce, and the Arms Export Control Act, administered by *
the Secretary of State through the ITAR, and (iii) other classified informa- *
tion for which the DOE, NRC, or other government department or agency has *
prescribed dissemination limitations. *

(1) Foreign representatives shall not be afforded access to *
classified information, unless specifically authorized in writing by a UA. *

1/ The following offices are responsible for processing visit requests; the *
Defense Intelligence Agency is responsible for processing requests to *
visit elements of the OSD, the Office of the Joint Chiefs of Staff *
(OJCS), the Unified and Specified Commands, the Defense Agencies, and *
activities administratively supported by the OSD. *

Department of the Army
Assistant Chief of Staff
for Intelligence
ATTN: Foreign Liaison
Directorate (DAMI-FL)
Washington, D.C. 20310

Department of the Air Force
International Affairs Division
Information Branch (CVAII)
Office of the Vice Chief of Staff
Washington, D.C. 20330

Department of the Navy
Foreign Disclosure and Policy
Control Branch
Office of Chief of Naval
Operations (OP-622E)
Washington, D.C. 20350

Defense Intelligence Agency
Foreign Liaison Branch (DI-4A)
Washington, D.C. 20301

(2) UA sponsorship of a visit is based on the existence of a specific or potential program or project with the foreign government concerned. UA notification of sponsorship will contain the level and scope of classified information authorized for disclosure (visual and/or oral only), as well as any limitations, and will be transmitted to the CSO for review and retransmittal to the contractor facility to be visited. Final acceptance of the visit will be subject to the concurrence of the contractor. The contractor shall notify the UA when the visit is not desired. The contractor may not change the level or scope of classified information to be released, or modify any limitations, without the approval of the UA which approved the visit.

(3) The contractor shall not inform the foreign representatives, or their employers, of the scope of access authorized or of the limitations imposed by the UA, nor shall the foreign representatives be induced to seek a higher access level than previously approved by the UA.

(4) The fact that a foreign representative may possess a PCL at a particular level does not automatically entitle the individual to receive U.S. classified information at that level.

(5) Prior to disclosure of classified information to foreign representatives, the contractor being visited shall advise such visitors of their continuing responsibilities to safeguard the information to be disclosed. The contractor shall also inform the visitors that the information affects the national defense of the U.S. within the meaning of the espionage laws of the U.S., and that unauthorized disclosure violates international agreements and is inimical to the interests of national security.

(6) If the UA declines to sponsor a visit, a declination notice will be furnished to the requesting embassy with an information copy to the security office of the contractor facility(ies) to be visited. A copy of the visit request will accompany the declination notice. Lack of sponsorship does not equate to disapproval nor does it preclude accomplishment of the visit, provided the contractor has, or obtains, a munitions license for the specific technical information proposed for release, or the information is otherwise exempt from the licensing requirements of the ITAR. Un-sponsored visits may be arranged between the foreign activity proposing the visit and the contractor. Disclosure of classified information during un-sponsored visits is prohibited: (i) without specific written authorization from the cognizant Military Department, or (ii) without a previously approved and current munitions license issued by the Department of State. It is the contractor's responsibility to consult applicable Department of State and Department of Commerce regulations to determine export licensing requirements or exceptions regarding the disclosure of unclassified technical data during visits by foreign representatives.

(7) In the event a UA denies a request to visit, the requesting embassy and the contractor(s) involved will be advised of the reason(s) therefor.

(8) The following subparagraphs pertain to reciprocally cleared contractors.

(a) Visit requests involving U.S. citizen employees of reciprocally cleared contractors (see paragraph 2-117) that require access to classified information or unclassified information related to a classified program or project, and all visit requests involving foreign national employees of such firms, shall be processed by the UA foreign disclosure office having jurisdiction over the information involved. To reduce administrative burden and facilitate the timely conduct of visits associated with current or potentially classified prime contractual or subcontractual relationships, contractors are encouraged to include as many activities to be visited as possible on each such request and propose that such visit request be approved on a recurring basis, preferably for the duration of the contract or subcontract involved. Copies of approved requests will be furnished by the contractor and to each contractor and UA activity approved for visitation. All subsequent changes to the list of visitors may be communicated by the requesting contractor directly to the activities to be visited, ATTN: Security Officer, making reference to the pertinent approved visit request on file. However, requests to visit activities not previously approved must be submitted separately to the cognizant foreign disclosure office for approval.

(b) Visits by U.S. citizen employees for unclassified commercial purposes may be arranged directly with the security office of the contractor or UA activity to be visited.

e. Category 5. Persons whose visits to a contractor's facility are considered necessary by the contractor, but who do not fall into other categories of this section, and who cannot be denied access to classified information by escort or other procedures, are included under Category 5. Only U.S. citizens are eligible to make visits in this category. *

(1) On receipt of the information specified in paragraph 41e, ISM, DISCO shall evaluate the request. If it decides to deny the request, it shall so advise the contractor. If DISCO determines that access is necessary and justified, it will initiate an appropriate investigation.

(2) The DISCO will review the investigative results and determine whether the visit authorization should be approved or denied. The DISCO will advise the contractor, in writing, of the authorization or disapproval of the visit, and DISCO will send an information copy to the CSO. LOC's shall not be issued for individuals in this visit category.

(3) On receipt of the information specified in paragraph 41e(3), ISM, for a renewal of a Category 5 visit authorization, DISCO shall reevaluate the need and justification for the renewal of the visit and advise the contractor of the authorization or disapproval of the request.

(4) DISCO will obtain assistance from the CSO, whenever necessary to resolve questionable reasons for access to classified information or justification for the visit.

3-104 Investigative Requirements.

a. The following requirements must be met before approval of Category 5 visits to contractors' facilities: U.S. citizens -- a BI with satisfactory results is necessary when TOP SECRET information is involved. A NAC with satisfactory results is required when SECRET or CONFIDENTIAL information is involved. *

b. Satisfactory completion of the investigative requirements established above shall not be evidenced by the issuance of the LOC or other forms of "clearance." The results of the investigation shall be recorded promptly in the PSCF through the submission of the DISCO Form 560 explaining the reason for the submission. *

3-105 RESTRICTED DATA. Visits involving access to RESTRICTED DATA shall be processed as follows.

a. Visits to a DoD or NASA contractor by a DoD or NASA representative or contractor shall be processed as prescribed in paragraph 3-103.

b. Visits to a DoD or NASA contractor by representatives of UA's other than the DoD and NASA and their contractors require prior approval of the DOE. The DOE Form F 5631.20 shall reflect this approval in part B of the form. Contractors submitting visit requests in this category shall, after certifying to the clearance status of the proposed visitor(s) in part A of the DOE Form F 5631.20, forward the form of the contracting officer for certification of the visitor's need-to-know and further processing in accordance with the UA's regulations. On receipt of a DOE Form F 5631.20, the contracting officer shall review the contractor's stated purpose for the visit. The contracting officer must assure him or herself that access to DOE classified information is essential to the performance of the DoD contract cited by the contractor, or that the proposed disclosure of classified information to the DOE activity will assist in either the performance of a DoD or a DOE contract. A statement to that effect shall be made in the appropriate part of the DOE Form F 5631.20. The necessary certification required on part A of the DOE Form F 5631.20 shall be made by the official of the UA who has been delegated this authority. In connection with contracts administered by a DCASR, the delegation of authority to make this certification is set forth in DLAM 5025.1 (reference (ss)). The request will also be reviewed to ensure that the prospective visitor has an appropriate PCL. When the PCL of a contractor is established, based on either a current classified contractual relationship or verification from the contractor's CSO, a cleared contractor's certification of the PCL of an employee shall be accepted without further confirmation by the DISCO. The contractor receiving a visit request in this category shall ensure that the required certifications have been made and that the visit has received DOE approval.

c. Visits to a UA contractor, other than a DoD or NASA contractor, by representatives of the contracting UA and between a prime contractor and his or her subcontractor on such a UA contract shall be processed as prescribed in paragraph 3-103.

d. Visits to a UA contractor, other than a DoD or NASA contractor, by representatives of UA's other than the contracting UA and by contractors other than under a prime-subcontract relationship shall require prior approval of the DOE and shall be processed in the manner prescribed in paragraph b above.

3-106 East-West Visit Exchange Program. If contacted by a UA relative to a proposed visit to a DoD cleared facility by representatives of a Communist country under the auspices of the State Department (East-West Exchange Program), the CSO shall furnish the following information 1/:

a. FCL status and safeguarding ability, and

b. adequacy of the facility's security program based on the most recent inspection, including a brief history of the program, such as past security violations or unsatisfactory ratings. If requested, the CSO will obtain the contractor's consent for the proposed visit and advise the UA accordingly.

Part 2. VISITS TO USER AGENCY ACTIVITIES

3-200 Application. This part outlines the procedures to be followed to process visit requests to UA activities where access to classified information is involved.

3-201 General Rules.

a. Contractors shall comply with any requests received from the commander or head of a UA activity for additional information needed in the processing of visit requests.

b. The contractor is encouraged at the time of the initial visit to request approval for subsequent visits within a period of 12 months, when necessary and consistent with the purpose of the initial visit. Arrangements for continuing visits will be made between the contractor and the Commander or Head of the UA activity. Final approval is the prerogative of the Commander or Head of the UA activity.

1/ The DoD wishes to be consulted in advance by any sponsor who intends either to discuss with the Communist country visitor research work which is funded by the DoD or to show any production having a direct military application. Consultation with the appropriate UA or CSO should have been completed before the itinerary is discussed with the Soviet and Eastern European Exchange Staff, Department of State. Access to industrial facilities performing on contracts, grants, or work funded by the DoD, classified or unclassified, or where the visitors will have access to production, having a direct or indirect military application, will not be granted without State Department approval, after consultation with the DoD.

c. Visits to DoD or NASA activities by DoD or NASA contractors involving access to RESTRICTED DATA shall be processed as prescribed in paragraph 3-103. Visits to other UA's involving access to RESTRICTED DATA shall be processed in the manner prescribed in paragraph 3-105b.

3-202 Visits to User Agency Activities in the United States.

a. Contractors desiring to have an employee or consultant visit a UA activity involving access to classified information shall address a request in writing to the Commander or Head of the activity to be visited. Visit requests shall be accompanied by a statement from the contracting officer that the release of classified information is required in connection with a specified classified contract or program. (Visit requests normally will be sent via the contracting officer.)

b. Requests to visit offices or headquarters activities of the UA's in the Washington, D.C. area shall be submitted in writing addressed to the specific office to be visited. Whenever possible, the exact code number, division, and branch of the activity or office to be visited shall be included in the address of the request. Visit requests shall be accompanied by a statement from the contracting officer that the release of classified information is required in connection with a specified classified contract or program. (Visit requests normally will be sent via the contracting officer.)

c. As an exception to paragraphs a and b above, a visit request may be submitted directly to the activity or office to be visited without a statement from the contracting officer when the classified information to be disclosed and the determination as to the contractor's need for such access is known to be a responsibility of the activity or office to be visited except as specified in paragraph e below.

d. The contractor's request shall contain the information specified in paragraph 37d, ISM.

e. If a contractor contemplates discussion or viewing of classified intelligence in the custody of a UA activity, the contractor's visit request shall be forwarded in all cases to the contracting officer of the UA activity authorized to release classified intelligence information to contractors for the required need-to-know verification and routing to the UA to be visited. In addition to the information specified in paragraph 37d, ISM, the visit request shall contain:

(1) the contractor's certification that access to classified intelligence is required for contract performance, and the contract is a classified contract;

(2) sufficient additional information concerning classified intelligence required to permit the agency or activity receiving the visit request to assess:

(a) applicability of available classified intelligence to the contractor's needs, and

(b) whether available intelligence may be released to the contractor without permission of the originator and/or sanitization of the material; and

(3) a certification by the contracting UA activity representative authorized to release classified intelligence to contractors, that the information to be acquired during the visit is not available within the sponsoring agency 2/.

(4) If the contractor's request is to visit the Defense Intelligence Agency (DIA), and it appears that a broad base of intelligence material may be examined or discussed during the visit, a knowledgeable representative of the sponsoring UA shall accompany contractor personnel during the initial visit.

3-203 Visits to User Agency Activities Outside the United States. This paragraph is applicable when a contractor desires to have an employee make a classified or unclassified visit to a UA activity outside the U.S. The information required by paragraph 37d, ISM, shall be furnished for the visits enumerated in this paragraph.

a. Contractor Sponsored Visits. A contractor shall process a request for his or her employee to visit a UA activity outside the U.S. through DISCO to the UA activity concerned, if the visit is on the initiative of the contractor. The DISCO will process the visit request to the appropriate activities based on guidance furnished from such activities (such as, major commands and Military Assistance Advisory Groups (MAAG's) attaches). The Commander or Head of the activity to be visited will notify the contractor of the approval or disapproval of the visit request. (See paragraph 3-401 for an employee based in Europe.)

b. User Agency Sponsored Visits. A visit request for a contractor employee sponsored by a UA and traveling on the UA's orders will be processed by the UA in accordance with the regulations of such UA. The traveler's order shall reflect the traveler's level of PCL, if required in connection with the travel. The contractor shall submit the request for such a visit directly to the UA activity concerned.

3-204 Action by Commander or Head of Activity to be Visited. The Commander or Head of the UA activity may --

a. Approve or disapprove the visit on the basis of the information provided, notifying the contractor accordingly, or request that the contractor furnish additional information in order to evaluate more fully the original visit request.

2/ The contracting officer, when verifying need-to-know, shall determine whether the required intelligence information is available locally or elsewhere within the UA, before authorizing visits to outside sources.

b. If there is reason to question the authenticity of the visit request or a need to verify the FCL status, the request shall be referred to the contractor's CSO for verification. Similarly, the request may be referred to the contractor's contracting activity if there is any question as to the justification for the visit or the visitor's need-to-know. When the FCL of a contractor is established, based on either a current classified contractual relationship or verification from the contractor's CSO, a cleared contractor's certification of the clearance of an employee visiting a UA should be accepted without further confirmation by the DISCO.

3-205 Compliance with Request from the Commander or Head of the User Agency Activity. As a result of the action taken by the Commander or Head of the UA activity as provided for in paragraph 3-204 -- the following actions shall be taken.

a. The CSO shall furnish as appropriate --

(1) To the contractor, the verification of the FCL and safeguarding ability or other requested information.

(2) To the Commander or Head of the UA activity, verification of the FCL and safeguarding ability or other requested information.

b. The contracting activity shall furnish, as appropriate --

(1) To the contractor, justification for the visit, or a statement that the visit cannot be justified.

(2) To the Commander or Head of the UA activity, justification for the visit, or a statement that the visit cannot be justified.

Part 3. VISITS TO GOVERNMENT ACTIVITIES OTHER THAN USER AGENCIES

3-300 Application. This part outlines the procedures to be followed to process visit requests to government activities other than UA's where access to classified information is involved.

3-301 Visits to DOE Installations or DOE Contractors.

a. Requests for visits to DOE installations or to DOE contractors which will require access to DOE classified information shall be prepared utilizing DOE Form F 5631.20. (Copies of this form may be obtained from any DOE installation). In addition to completing the appropriate portions of the DOE Form F 5631.20, the contractor (usually the FSO) shall include, in the first block of the form immediately after the PCL data, a certification of the prospective visitor's PCL. The DOE Form F 5631.20 shall then be forwarded for the required official certification to the contracting officer of the UA who signed the DD Form 254 which was issued in connection with the contract for which the DOE classified information is required.

b. On receipt of a DOE Form F 5631.20, the contracting officer shall review the contractor's stated purpose for the visit. The contracting

officer must assure him or herself that access to DOE classified information is essential to the performance of the DoD contract cited by the contractor, or that the proposed disclosure of classified information to the DOE activity will assist in either the performance of a DoD or DOE contract. A statement to that effect should be made in the appropriate part of the DOE Form F 5631.20.

c. The necessary certification required on part A of the DOE Form F 5631.20 shall be made by the official of the UA who has been delegated this authority. In connection with contracts administered by a DCASR, the delegation of authority to make this certification is set forth in DLAM 5025.1 (reference (ss)).

3-302 Visits to Activities Other Than the Department of Energy. Requests for visits to government activities other than UA's and the DoE, which involve the release of classified information to such activities in connection with a UA contract, require the approval of the contracting officer, and, if the classified information to be released includes RESTRICTED DATA, the approval of the DOE. Such requests shall be submitted by the contractor to his or her contracting officer who will process the requests in accordance with the internal instructions of the department or agency. Before approving a contractor's request to disclose or acquire classified information during such a visit, the contracting officer should require evidence from the contractor that the activity to be visited had requested or else consented to the contractor's request for the visit. Also, the contractor should submit a statement explaining:

- a. the purpose of the visit in detail;
- b. a description of the classified information to be divulged during the visit, either to or by the government activity being visited; and
- c. the direct or indirect effect that the visit may have on the performance of the classified contract involved.

Part 4. VISITS TO FOREIGN GOVERNMENTS AND ACTIVITIES

3-400 Application.

a. Contractor visits to foreign governments or activities or to international bodies fall into three categories.

(1) These include visits which involve the disclosure of U.S. classified information:

(a) in connection with a government-to-government agreement to furnish U.S. military equipment to the foreign government (for example, when the purchase of the equipment is under a U.S., not a foreign government, contract);

(b) in connection with exploratory sales visits involving precontract negotiations or contract performance, other than those covered under paragraph (a) above, (for example, when the purchase of the U.S.

military equipment or services, if consummated, will be under a foreign government contract); or

(c) in connection with U.S. Government presentations to foreign governments and international pact organizations when the U.S. Government has requested the contractor's participation.

(2) These include visits which do not involve disclosure of U.S. classified information but for which the foreign government or activity requires a U.S. security assurance on the visitor:

(a) which involve disclosure of unclassified technical data on the "U.S. Munitions List," or

(b) which will not involve disclosure of technical data on the "U.S. Munitions List."

(3) These include visits on a commercial basis (for example, visits that do not involve disclosure of U.S. classified information and do not require a U.S. security assurance on the visitor). These visits may or may not involve disclosure of unclassified data on the "U.S. Munitions List." Visits in this category are not processed under the provisions of this regulation. However, the contractor is responsible for compliance with the ITAR (reference (i)) and for obtaining a State Department export license or letter, if required.

b. The following information concerning the requirements of reference (o) is furnished for the guidance of the contractor.

(1) Disclosure of classified information, in connection with visits in the category described in paragraphs (1)(a) and (c) above, does not require an export license.

(2) Except as specified in paragraph (3) below, disclosure of unclassified technical data related to "U.S. Munitions List" items requires an export license.

(3) An export license is not required if the visit has been approved on an unclassified basis by the UA concerned and (i) the technical data to be disclosed is information covered by a manufacturing license or technical assistance agreement approved by the Department of State or (ii) the technical data to be disclosed is exempt from the provisions of the ITAR (reference (i)).

c. Requests for classified visits to foreign governments or activities shall be processed only for employees who have a PCL for the appropriate level. Contractor-issued CONFIDENTIAL clearances are not valid for such visits.

d. Visit requests in the categories described in paragraphs a(1)(b) and a(2)(a) and (b) shall be processed by the contractor through DISCO. Visits in the category described in paragraphs a(1)(a) and (c) above, shall be processed by the contractor in accordance with the regulations of the UA which cover dealing with the foreign government. The contractor shall

certify clearance information concerning the proposed visitor directly to the UA concerned. Such visits are not processed through DISCO.

e. Visit requests processed through DISCO shall be submitted in quadruplicate with one extra copy for each additional country to be visited, and shall contain the information required in paragraph 37d, ISM, as well as the proposed visitor's passport or identification card number, date, and place of issuance. In addition, the contractor shall specify the category of visit which is involved (see paragraph a above), and, for a visit of the type described in paragraph a(1)(b) or a(2)(a) above, will certify, within the visit request, the export license number and license expiration date 3/. *
The DISCO shall review the visit request to ensure that it is complete and accurate and contains the necessary information to process the visit. The visit request will then be forwarded to the OISI, MAAG, Attache, or Unified Command as appropriate. These latter activities will arrange the visit with the foreign activity to be visited and advise the contractor directly of approval or disapproval of the visit. In every case the disclosure authorization, letter or license, shall be forwarded to the U.S. Government point of contact in the foreign country. *

f. Processing Time. Visit requests should be received by DISCO at least 45 days in advance of the proposed travel date for all countries and U.S. overseas commands. Exceptions are travel to Switzerland which requires 70 days advance notice. Requests for visits in France must be for specific dates as France will not approve visits for indefinite periods.

3-401 Use of OISI. If the U.S. contractor employee making the visit is based in Europe, or in an adjacent non-European country, the visit request may be submitted through OISI rather than through DISCO. The information required in paragraph 3-400e above shall be included with the request. The OISI will verify the proposed visitor's PCL status and process the visit to the foreign activity to be visited. The OISI will notify the contractor of the approval or disapproval of the visit. In addition to furnishing a copy of the export license or letter when required in accordance with paragraph 3-400e, the contractor is responsible for compliance with the ITAR (reference (1)), if applicable, in the same manner as though the visit were arranged through DISCO.

Part 5. VISITS IN CONNECTION WITH BILATERAL INDUSTRIAL SECURITY AGREEMENTS AND NATO VISIT PROCEDURES

3-500 Visits in Connection With Bilateral Industrial Security Agreements.

a. The following procedures apply to visits pertaining to precontract negotiations or contract performance under approved bilateral agreements involving a foreign classified contract in the U.S. or a U.S. classified contract in a foreign country.

3/ To avoid delay in obtaining visit approval, the contractor should obtain any required export license or letter well in advance of the proposed visit.

(1) Authorization for visitors or those visited to have access to classified information shall be limited to that necessary for official purposes in connection with precontract negotiations or contract performance. When requested, the authority to visit the facility of the prime contractor may include authorization to have access to or to disclose classified information at the facility of a subcontractor engaged in performance of work in connection with the same contract.

(2) A list may be developed to indicate those individuals who are authorized to visit the facility for extended periods of time, not to exceed 6 months, as may be necessary in the performance of the contract. This authorization may be renewed for additional periods of 6 months as may be necessary in the performance of the contract.

(3) Visits shall be approved only for persons possessing government-granted PCL's.

b. U.S. contractor visits in connection with foreign classified contracts shall be processed in accordance with the provisions of paragraph 3-400.

c. Representatives of foreign governments visiting U.S. activities shall be processed as Category 4 visits in accordance with paragraph 3-103d, if U.S. classified information is involved in the foreign government's contract. If only foreign classified information is involved, the visit shall be processed by DISCO.

3-501 NATO Visit Procedures. The following visitor control procedures apply to a NATO precontract negotiation or to a NATO contract awarded to a U.S. contractor by a NATO government other than the U.S., a contractor of such NATO country, or a NATO international body.

a. Visits by Representatives of a U.S. Contractor to the NATO Contracting Officer, a NATO Management Office, or a Contractor of a NATO Country Other Than the United States. The visit request, in quadruplicate, will be directed through DISCO to the NATO contracting officer or to the NATO management office and will be processed together with a Certificate of Security Clearance (see paragraph 3-503). The Certificate of Security Clearance shall indicate whether or not the visitor has received a NATO security briefing 4/. The visit request shall include the information specified in paragraph 37d, ISM, the visitor's passport or identity card number, date and place of issuance, and the NATO contract or program on which he or she is engaged.

4/ Whenever possible, the NATO security briefing will be accomplished prior to the submission of the visit request and the certificate will state so. When this is not practical, the visit request will include a statement as to when and by whom the NATO security briefing will be conducted.

b. Visits by Representatives of a NATO Contracting Officer, a NATO Management Office, or of a Contractor of a NATO Country to the U.S. Contractor. Such requests shall be processed by the NATO activity concerned as a Category 4 visit (see paragraph 3-103d) through the appropriate UA activity. Such visit requests shall contain the information specified in paragraph a above.

c. Visits in Connection with NATO Contracts by Representatives of a U.S. Contractor to Another U.S. Contractor in the United States.

(1) Such visits shall be processed as Category 1 visits (see paragraph 3-103a) if both contractors are performing on the same NATO contract in a prime contractor-to-subcontractor relationship. A statement on NATO security briefing shall be included in the visit request.

(2) If no contractual relationship exists between the contractors, the visit request shall be processed as a Category 2 visit (see paragraph 3-103b) requiring the approval of the NATO contracting officer whose information is involved. Supporting information on the NATO briefing and the Certificate of Security Clearance shall be included in such visit requests. The visit request, together with two copies of the Certificate of Security Clearance, will be processed through DISCO to the NATO Contracting Officer.

d. Recurring Visits. Subsequent visits shall be processed in accordance with paragraph 3-101. Authorization for subsequent visits shall not exceed a period of 12 months, but may be subject to renewal for succeeding periods of 12 months, if required.

3-502 NATO Production Logistics Organization (NPLO) Program Security Clearance and Visit Procedures. Clearance and visit control procedures in effect for contractors performing on specific NPLO programs are different from other NATO visit procedures. Current NPLO programs are HAWK, F-104G, NAMSA, and NICSO. As an aid to simplify visit procedures, it is necessary to establish the visiting contractor employee's PCL in connection with a specific NPLO program. This may be accomplished prior to the initial visit or concurrent with the request for such visit.

a. Initial Visits.

(1) The visit request, in quadruplicate, will be directed through DISCO to the NPLO Management Office with a copy to the NATO activity to be visited and will be processed together with a Certificate of Security Clearance (see paragraph 3-503). The visit request shall include the information specified in paragraph 37d, ISM, the visitor's passport or identity card number, date and place of issuance, and the NPLO program with which he or she is concerned.

(2) The DISCO will forward the visit request to the Management Office of the NPLO which will inform appropriate NATO and foreign activities of its action, for example, approval or disapproval.

(3) The Certificate of Security Clearance will be forwarded by DISCO to the NATO Office of Security Industrial Security Section for recording and dissemination of the information to the NATO member countries and NPLO Management Offices concerned.

(4) In case of urgency when a Certificate of Security Clearance has not been forwarded to the NATO Office of Security in advance, DISCO will attach a copy of the Certificate of Security Clearance to the visit request for transmission to the NPL0 Management Office.

b. Recurring Visits. If the initial visit is approved, subsequent visits, not to exceed 6 months, to the same NPL0 activity for the same U.S. contractor employee will be processed by the U.S. contractor directly to the NPL0 activity to be visited. That activity will notify the contractor of the approval of the visit. These subsequent visit requests will contain the information required by paragraph 37d, ISM, and will include the visitor's passport or identification card number and date and place of issuance.

3-503 Certificate of Security Clearance.

a. A standard format, Certificate of Security Clearance, has been adopted for use within the NATO community in connection with visits from one NATO country to another, or to a NATO office, agency, command, or to or between contractors when a visit will involve access to NATO classified information.

b. The Certificate of Security Clearance shall be completed on plain bond paper by the contractor for each of his or her employees desiring to make a visit, and submitted in duplicate for certification to DISCO. The employee's name shall be listed in the following order: last name, first name, and middle name or initial.

c. This certificate shall be sent sufficiently in advance by the contractor through DISCO so as to assure receipt by the foreign officials of the NATO offices, agencies, commands, or contractors before arrival. In exceptional circumstances, the information required by the certificate may be initially supplied by other means of communication, but shall be confirmed in writing. Normally a copy of this certificate should not be given to the traveler.

d. The DISCO shall forward the Certificate of Security Clearance to the OISI. That office processes the certificate to the appropriate NATO contracting activity. When the appropriate briefing has not been administered, the OISI will administer the NATO security briefing only if the visitor is located in or is in transit through Brussels. If it is more convenient, the briefing may be administered by a U.S. UA activity if specifically requested to do so by a contractor.

DEFENSE INDUSTRIAL SECURITY CLEARANCE OFFICE
DEFENSE INVESTIGATIVE SERVICE

Certificate of Security Clearance

Issued by _____

Date and place of issue _____

_____ valid until _____

(If issued to an individual, this certificate should be returned to the granting authority on the termination of the mission for which issued.)

This is to certify that: _____
(Last name, first name, middle name)

Date of birth _____

Place of birth _____

Nationality _____

Where employed _____

Programme(s) _____

Holder of passport and identification card number _____

Issued at _____

Military rank and number (if applicable) _____

_____ has been cleared for access to information classified up to and including _____

_____ in accordance with current NATO security regulations. This individual

(Has) (Has not) received a NATO security briefing.

Signature and title of granting authority
(Seal or stamp)

SECTION IV. SECURITY INSPECTIONS**Part 1. INSPECTIONS**

4-100 **Application.** This part sets forth the purpose and establishes the procedures and schedule for the conduct of industrial security inspections.

4-101 **Purpose.** Security inspections shall be conducted for all cleared contractor facilities having access to classified information to ensure compliance with the requirements of the DoD Industrial Security Program. Such inspections shall ensure that procedures, methods, and physical safeguards employed by contractors are adequate for the protection of classified information entrusted to them. In addition, the inspection shall serve as a method for providing recommendations and suggestions to improve security practices at the facility.

4-102 **Reciprocal Use of DOE and DoD Security Inspection Programs.** Existing security inspection agreements between CSO's and DOE activities, whereby CSO's perform inspections of DOE classified contracts at DoD-cleared contractor facilities or the DOE agrees to perform inspections of DoD contracts which may or may not involve RESTRICTED DATA at DOE facilities, will continue to be honored. However, such agreements should be reviewed and updated as necessary to conform with the general policy outlined in this paragraph. Copies of revised and new agreements entered into subsequent to the receipt of this regulation, shall be furnished the Director, DIS, ATTN: Deputy Director (Industrial Security).

a. A DoD CSO may, on receipt of a request from a DOE activity, enter into a written agreement to assume security inspection responsibility for a DOE classified contract being performed at a DoD cleared contractor's facility. The requesting DOE activity shall be responsible for notifying the contractor that the provisions of the ISM 1/ will apply to the DOE contract and that the security inspections will be performed by the contractor's present DoD CSO. The DoD CSO will be responsible for:

(1) initially notifying the DOE requesting activity of the contractor's FCL and safeguarding ability, and the mailing address to which DOE classified material should be addressed;

(2) subsequently notifying the DOE requesting activity of any contemplated termination or revocation of the contractor's FCL, inability to safeguard the DOE classified information, or change in mailing address;

(3) ensuring that the DOE interests are covered during recurring inspections -- normally, copies of the DD Form 696 shall not be furnished the interested DOE activity; however, if requested upon initial award of a DOE contract or whenever an unsatisfactory security rating is assigned, a copy of the DD Form 696 shall be furnished; and

1/ If there are any exceptions, both the contractor and the DoD CSO shall be advised in writing.

(4) advising the interested DOE activity of any serious security deficiencies encountered or any case involving loss, compromise, or suspected compromise of classified information pertaining to the DOE contract. Such advice may be in the form of a copy of the letter to management, a copy of the investigative report of loss, compromise, or suspected compromise, or a synopsis of the overall status of security in the facility, including those deficiencies that specifically affect the DOE contracts.

b. A DoD CSO may enter into a written agreement with a DOE activity to perform certain DoD security cognizance actions when a DoD contract is being performed at a DOE cleared contractor's facility. In such cases, the security actions and responsibilities of the DOE activity and the DoD CSO shall be included in the DOE/DoD Agreement.

(1) The DOE activity shall be responsible for the following.

(a) Notify the CSO of any contemplated termination of DOE interest at the contractor's facility, or inability of the contractor to safeguard the DoD classified information, or any changed condition that would affect the contractor's DoD FCL (see paragraph 2-118).

(b) Assure that the DoD interests outlined in the written agreement are covered during security inspections. Normally, copies of the DOE inspection report shall not be furnished the DoD CSO. However, if requested on initial award of a DoD contract or whenever an unsatisfactory security rating is assigned, a copy of the DOE inspection report shall be furnished.

(c) Advise the DoD CSO of any serious security deficiencies encountered or any case involving loss, compromise, or suspected compromise of classified information pertaining to the DoD contract. Such advice may be in any appropriate form or format (see paragraph a(4) above).

(2) The DoD CSO shall be responsible for the following.

(a) Process and issue a DoD FCL in the normal manner to enable the contractor to bid on other classified DoD contracts.

(b) Advise the DOE activity of those paragraphs in the ISM that are either in addition to or different from DOE requirements and which should be covered by the DOE activity during inspection. For example, ensure that the contractor complies with sections V and VI and paragraphs 5, 6, 7, 10, 14, and 17, ISM 2/. Except as indicated, the DOE security requirements apply.

(c) As appropriate, arrange with DISCO to process personnel actions for individuals requiring a FCL in connection with the FCL and issuance

2/ The paragraphs of the ISM in the examples apply in all cases. However, based on the specific case at hand, there could be additional paragraphs of the ISM which should be delineated.

of a DoD LOC. In addition, personnel requiring access to DoD TOP SECRET information shall be cleared by DISCO and issued a DoD LOC. However, access to DoD SECRET information may be granted within the facility on a strict need-to-know basis without being issued a DoD LOC, provided the employee has a "Q" clearance. If the employee does not have a "Q" clearance or requires access outside the facility (for example, on visits), he or she shall be cleared by DISCO and issued a DoD LOC. Access to CONFIDENTIAL information may be granted based upon a contractor's CONFIDENTIAL clearance except as noted in paragraph 24, ISM.

(d) Notify the contractor in writing of the agreement reached with the DOE activity and also advise the contractor of his or her security responsibilities with specific emphasis on those items included in the DOE/DoD agreement in accordance with the two preceding paragraphs.

(e) Maintain liaison with the DOE activity immediately prior to and subsequent to the award of a DoD contract and upon completion or termination of the DoD contract to assure that all DoD requirements are complied with by the UA and the contractor.

4-103 Schedule. An initial inspection, in addition to the visit required by paragraph 1-110c or 1-111b, shall be completed within 20 days from the time the CSO receives notice that the facility has classified material in its possession, but in any event, within 2 months from the date of the FCL. Initial inspection of a COMSEC account shall be made jointly with a representative of the COR. Inspections of contractor facilities shall be conducted in accordance with the schedule indicated below. This schedule does not preclude conducting inspections on an unannounced basis or at more frequent intervals wherever conditions at facilities dictate or when otherwise warranted. As an example, serious deficiencies encountered in a facility's security program would indicate a need for increased inspection effort. When an unannounced inspection is conducted, some of the administrative data normally furnished by the contractor, and entered on the DD Form 696, may not be available. In such cases, the information may be omitted from the DD Form 696, but shall be included at the time of the next announced inspection. In instances in which the contractor reports to the CSO the establishment of or any change in the location of a closed or restricted area within the facility, the CSO shall determine if it is necessary to make an inspection prior to the next regular inspection. Such determination should be based on the CSO's previous experience and knowledge of the contractor's operation plus an evaluation as to the contractor's past dependability in safeguarding classified material while an area is being established. In these instances where parent and subsidiary facilities have entered into approved formal agreement as provided for in paragraph 72c, ISM, both facilities shall be inspected simultaneously.

a. The inspection schedule shall be based upon the highest level of classified material possessed at the facility since the preceding inspection except as otherwise provided below.

b. Inspection Schedule.

| (1) <u>Level of Possession</u> | <u>Frequency</u> |
|--------------------------------|------------------|
| TOP SECRET | 6 months |
| SECRET | 6 months |
| CONFIDENTIAL | 9 months |

- (2) All other facilities, except
as noted below

9 months

c. It is the responsibility of the Deputy Director (Industrial Security), HQ DIS to ensure that specific unannounced inspection standards and criteria be developed and that they be uniformly applied throughout each CSO. Unannounced inspections shall be approved in advance by the cognizant Director of Industrial Security, his or her designee, or higher authority.

d. The inspection schedule for facilities which are candidates for administrative termination may be lengthened or shortened to accommodate the requirements of paragraph 2-119.

e. HOF's of commercial carriers and their terminals listed on the DIS Form 1150 which have been granted a FCL will be inspected every 6 months.

f. Graphic arts facilities will be inspected every 6 months.

g. CSO's will arrange to inspect periodically selected uncleared locations where cleared personnel are employed or physically located to verify the continuing adequacy of the alternative procedure to annual visits provided for in paragraph 73, ISM.

h. CSO's will, in conjunction with performing regularly scheduled industrial security inspections, conduct OPSEC inspections to assess contractor compliance with UA imposed OPSEC requirements. Section X provides further guidance on these type inspections. *

4-104 Notification of Inspection.

a. Prior to visiting a facility for the purpose of a recurring inspection, the facility shall be notified approximately 10 days in advance of the impending visit. This, in addition to being a common courtesy, affords the FSO an opportunity to prepare for the inspection. For instance, he or she has to verify that representatives of management will be available for discussions and for the post inspection critique, and that other key personnel such as the document control supervisor, contract administrator, and reproduction supervisor will be available for interview. Finally, the contractor needs sufficient time to prepare a list of classified contracts on which the facility is currently performing.

b. Prior to effecting an inspection at a contractor facility, the inspector shall accomplish the following.

(1) Review the previous DD Form 696, related correspondence, and any subsequent reports. Deficiencies recorded on the preceding DD Form 696 report should be noted and the extent of corrective action checked during inspection. Failure to correct the deficiencies during the interval between the inspections shall be discussed with management to determine its attitude toward its security program.

(2) Review the list of current classified contracts, the DD Forms 254, and related forms. This review will, in addition to indicating the highest classification of material that should be in the facility, reveal

whether or not classified material in the form of hardware or equipment is to be produced. If so, the inspector should be alerted to the fact that there would, or should be, controlled areas to be inspected at the facility. Note the dates shown on the DD Form 254 for evidence of failure on the part of the contracting activity to conduct required biennial reviews. In each instance the DD Form 254 should be reviewed carefully prior to the inspection. *

(3) Take note of any special access requirements or other additional security requirements for particular contracts.

(4) Review any reports of recent security violations. Reports submitted by the facility under paragraphs 6a(2) and (3), ISM, should be screened. An excessive number of such reports, particularly if they are similar in nature, would indicate a laxity in the facility's document control system, educational program, or both. Absence of such reports is also worth noting. If the loss of documents or other indications of compromise are detected during the inspection (when it is established that the facility has prior knowledge of these conditions), this would be an indication of failure to comply with the ISM reporting requirements.

(5) Review the facility's SPP to ensure that it provides a complete set of adequate procedures which specify what is to be done, how it is to be done, who is to do it, and who is to supervise it. If there are omissions in the SPP, or if the SPP has not been set forth in sufficient detail, it is likely that deficiencies will be discovered during the inspection in the same areas in which the procedures are silent or covered in general terms. Note also if the last revision to the ISM has been incorporated into the procedure.

c. If plant representatives or their designees are at the facility (including a DCASR plant representative), they shall be alerted to the forthcoming inspection and visited as soon as possible after arriving at the facility. In addition, every effort shall be made to brief the plant representatives or their designees of the inspection results in advance of the briefing to be given to management. If the plant representatives or designees are not available, they will be apprised of the inspection results as soon as possible, after conclusion of the inspection, by copies of correspondence. An invitation shall also be extended to the plant representatives or their designees to attend the management critique and they shall be placed on distribution for copies of correspondence subsequently sent to management relative to the inspection.

d. In those instances where the CSO elects to perform an inspection on an unannounced basis as provided for in paragraph 4-103, the notification provisions outlined above will not apply.

4-105 Use of Industrial Security Inspection Report (DD Form 696). This form is designed to focus attention on the security requirements established in the ISM and DoD 5220.22-S-1 (reference (q)), as well as to serve as a guide for the conduct of security inspections. When filled in, the original of the form shall be maintained by the CSO in the facility file folder in order to have available the latest information for the evaluation of the current security status of the facility. The completed forms are not routinely distributed to UA's or the contracting officers having procurement

responsibilities at the facility; however, the CSO shall, on request, furnish advice as to the latest security conditions of the facility. A DD Form 696 is generally useful to the UA's only when the facility has been evaluated as "unsatisfactory." In such cases the CSO will automatically furnish a copy of the DD Form 696 to every contracting activity concerned, under the provisions of paragraph 4-201.

4-105.1 TEMPEST Countermeasures.

a. DoD policy requires contractors to take TEMPEST countermeasures only if such special security requirements are specifically incorporated into the contract by the UA whose classified information is processed. A copy of these special security requirements shall be furnished the CSO by the UA.

b. Contracting officers shall ensure that potential compromising situations related to the performance of classified contracts are identified and evaluated, and, where appropriate, include in such contracts requirements for the security countermeasures necessary to ensure compliance with national policies for the control of compromising emanations. When such contract requirements are established, the CSO shall be advised.

c. The CSO may obtain technical assistance from the contracting officer or his or her designated representative when necessary in connection with the inspection of a contractor's facility for compliance with TEMPEST countermeasure provisions of the contract.

d. In those instances where the UA has not incorporated special security requirements as TEMPEST countermeasures in the contract, and the CSO believes such measures are warranted, the CSO should bring the matter to the attention of the appropriate contracting officer. If more than one UA utilizes the equipment, the issue should be discussed with all contracting officers whose classified information is being processed. Factors to be considered by the CSO will be: (i) the type of equipment or component involved, (ii) the physical environment in which the component is located, (iii) the sensitivity of the classified information, and (iv) the frequency, volume, and duration of classified information processing.

e. Contracting officers should direct any questions concerning TEMPEST policy or countermeasures to the following activities.

Director
National Security Agency
ATTN: S6
Fort George G. Meade, MD 20755

Commander
U.S. Army Intelligence & Security Command
ATTN: IAOPS-OP-P
Arlington Hall Station
Arlington, VA 22212

U.S. Air Force Cryptologic Support Center
ATTN: EPV
San Antonio, TX 78243

Commander
Naval Security Group Command
ATTN: G-65
3801 Nebraska Ave., NW
Washington, D.C. 20390

4-106 Use of the DIS Form 1148. This is a multipurpose form designed to focus attention on the security requirements established for commercial carriers.

a. The purpose of part I is to develop sufficient facts and to ensure submission of necessary documents to permit an administrative determination to grant or deny a security clearance to a HOF and terminals listed on the DIS Form 1150 of a commercial carrier. It is also the basis for a CSO of the HOF of a carrier to determine if the overall carrier organization should be granted authority to transport SECRET material. In addition, part I is utilized to develop information concerning changed conditions, such as a change of address or reorganization. Part I is also to be used by the CSO in determining whether the HOF of the commercial carrier is subject to FOCI factors. The information in part I and attachments thereto is used as an aid to investigation in such cases. Whenever part I is used, the original of the form with all attachments will be forwarded to DISCO. The CSO will retain a copy in its facility file folders.

b. The purpose of part II, when used in conjunction with the applicable inspection check list, is to provide for uniform and comprehensive security inspections of cleared facilities of commercial carriers to determine compliance with the requirements of reference (b), as well as the ISM, as appropriate. When part II is used, the CSO will retain a copy in appropriate facility file folders in order to have available the latest information pertaining to the security status of the facility inspected. In addition, the CSO of the HOF will be furnished and will retain copies of reports and correspondence pertaining to violations or major deficiencies (including unsatisfactory reports) for all of the carrier's terminals in order to have available the latest information pertaining to the overall security status of the carrier's organization (system). As necessary, the CSO of the HOF will assist other CSO's over terminals in obtaining satisfactory corrective action from top management officials of the HOF. The information in part II is not intended for routine distribution; however, the CSO shall, on request, furnish advice as to the security status of the commercial carrier.

c. Instructions governing the use of this form are contained in paragraph 9-206.1.

4-107 COMSEC Inspections.

The purpose of the inspection of a COMSEC account is to determine whether contractors are complying with the requirements of reference (q) and such additional security requirements as may be provided for by the individual contracts for the safeguarding of COMSEC information. The inspection is designed to obtain an overall security evaluation of the facility's protection of COMSEC information and the current security status of COMSEC information in the facility. Following each COMSEC inspection, the CSO shall provide a report of the inspection to the appropriate COR.

*
*
*
*
*
*
*

Formal Notification.

a. The contractor shall be notified in writing of the results of the inspection. The letter shall be addressed to management and not to the FSO. A copy of this letter may be sent to the FSO. While a basic format for these letters is acceptable, each should be a typed letter rather than a printed form. The notification shall identify all significant security deficiencies noted during the inspection with specific reference to the appropriate paragraphs of the ISM. The facility shall be given a specific date by which all deficiencies cited shall be corrected, and requested to notify the CSO when the corrections have been accomplished.

b. Depending on the severity of the deficiencies and the known reliability and attitude of the facility, the CSO may either conduct a special inspection to determine whether the deficiencies have been corrected or accept management's written statement that the corrective action has been accomplished subject to verification at the next inspection.

Part 2. UNSATISFACTORY INSPECTIONS

4-200 Application. This part establishes procedures to be followed in instances of unsatisfactory security inspections, or whenever there is an immediate danger of classified information being compromised.

4-201 Procedures.

a. If a CSO determines that there is an immediate danger of classified information being compromised ^{3/} or if a security inspection conducted under the provisions of part 1 of this section results in an overall facility security evaluation of "unsatisfactory," the CSO shall notify immediately the Regional Director and the Director, DIS, ATTN: Deputy Director (Industrial Security), of all pertinent facts. That office shall also be kept informed of all subsequent developments. In addition, the actions described below shall be taken.

(1) The Regional Director shall notify the contractor that the existing deficiencies shall be corrected within the period of time prescribed (not to exceed 30 days) and of the possible consequences if satisfactory action is not taken. Include in the letter to the contractor a statement that the contracting activities have been notified of the existing conditions.

(2) Within 3 days from the completion of the inspection, notify by electrical message the contracting officer(s) concerned of the nature and scope of the deficiencies, the specific contracts which are

^{3/} In every case where there is immediate danger of classified information being compromised, require the contractor to take immediate measures to safeguard the classified information. If the contractor refuses or is unable to take immediate corrective action, the CSO shall recover, or arrange with the contracting officer(s) concerned, for the recovery of the classified information.

affected, the action taken by the contractor to remove the danger of compromise, if any, and the contractor's plan to correct the deficiencies and the scheduled date for completion. (Actions by the contracting officer(s) are not required at this time.)

(3) Conduct reinspection immediately following the end of the period prescribed for correction of the deficiencies to determine whether necessary corrective action has been taken or whether an additional period of time should be granted in which to complete the corrective action. If the CSO is satisfied that management has taken adequate action to correct the deficiencies, electrical message notification of the "satisfactory" evaluation will be sent to the same addressees who received the notification as to the "unsatisfactory" evaluation.

b. If there is no immediate danger of compromise of classified information but the contractor nevertheless has failed to correct the deficiencies within the allotted period (or any extension thereof), the Director of Industrial Security shall notify the contracting officer(s) concerned, each contractor having a classified subcontract in the facility, and each contracting UA ^{4/} that the release of additional classified information to the facility should be withheld, except for information necessary to the completion of essential contracts. In addition, such notification should also state that the facility is considered ineligible to receive requests for proposals or invitations to bid on or for the award of new classified contracts. A copy of this notice shall be furnished the DUSD(P), ATTN: DSP&P through the Director, DIS. The contracting UA shall determine whether to terminate existing classified prime contracts or whether the overall defense interest requires their completion.

4/ As appropriate, notices to contracting UA's specified in this paragraph shall be addressed as follows:

Assistant Chief of Staff for Intelligence, USA, ATTN: DAMIDOS,
Washington, D.C. 20310
Chief of Naval Operations, Director of Naval Intelligence, ATTN: 009D,
Washington, D.C. 20350
Director of Security Police, USAF, ATTN: IGSPA, Washington, D.C. 20335
Director of Security, NASA, ATTN: Code LZ, Washington, D.C. 20546
Chief, Security & Investigations Division, Small Business Administration,
Washington, D.C. 20416
Security Officer, National Science Foundation, Washington, D.C. 20550
Director of Investigations and Security, Department of Transportation,
Washington, D.C. 20590
Security Office, Department of the Treasury, Washington, D.C. 20220
Chief, Division of Enforcement and Security Management, Department of
Interior, Washington, D.C. 20240
Department Security Officer, Department of Agriculture, Washington, D.C.
20250
Chief, Physical Security Division, United States Information Agency,
Washington, D.C. 20547

When classified subcontracts are involved the ACO will make this determination after appropriate coordination, and advise the concerned prime and subcontractor if the classified subcontract is to be terminated. If, on completion of existing contracts, the security deficiencies have not been corrected, take the action prescribed in paragraph c below, unless it has been previously taken.

c. When a contractor persistently fails or refuses to discharge his or her obligations under the "Department of Defense Security Agreement" to protect classified information, the CSO shall recommend to the Director, DIS, ATTN: Deputy Director (Industrial Security), through the Regional Director, the revocation of the FCL. That office shall make all reasonable efforts to secure the compliance of the contractor. If these efforts are not successful, the Director, DIS, after consultation with the concerned contracting officer(s) and contracting UA's, shall authorize the CSO through the Regional Director to revoke the facility clearance (see paragraph 2-121). Copies of such authorizations will be furnished to DSP&P.

d. When an authorization to revoke a FCL is received the CSO shall:

(1) immediately notify each contractor having a classified subcontract in the facility that the subcontractor's FCL is being revoked and that he or she, as a prime contractor, shall without delay submit a listing of existing classified subcontracts in the facility to the contracting officer(s) concerned, requesting instructions with respect thereto;

4/(Continued)

Director of Investigations and Security, Department of Commerce, Room 5004, Main Commerce Building, Washington, D.C. 20230

Director of Investigations, General Services Administration, Washington, D.C. 20230

Director of Security, ATTN: SY/DO, Department of State, State Department Bldg., Washington, D.C. 20230

Director, Investigations and Security, Office of the Assistant Secretary for Administration, Department of Labor, Washington, D.C. 20210

Director, Security and Inspections Staff, Environmental Protection Agency, Washington, D.C. 20460

Director, Office of Safeguards & Security, U.S. Department of Energy, Washington, D.C. 20545

Director, Security and Administrative Programs Staff, Office of Management and Finance, Department of Justice, Washington, D.C. 20530

Security Officer, U.S. Arms Control and Disarmament Agency, Washington, D.C. 20451

Security Officer, Federal Emergency Management Agency, 1725 I Street, NW, Washington, D.C. 20472

Director, Office of Security and Safety, U.S. General Accounting Office, Washington, D.C. 20548

Chief of Security, Board of Governors, Federal Reserve System, 20th and C Streets, N.W., Washington, D.C. 20551

(2) recover, or arrange with the contracting officers(s) concerned for the recovery of all classified information; and

(3) after all classified information has been recovered:

(a) terminate the contractor's DD Form 441 in accordance with section IV of the agreement,

(b) withdraw the DIS FL 381-R,

(c) forward a DIS Form 553 to DISCO annotated to indicate revocation of the FCL on grounds pertaining solely to the physical elements of security, and

(d) forward a copy of DIS Form 553 reflecting the revocation action to the DTIC.

4-202 Unsatisfactory Evaluation of a Commercial Carrier.

a. Whenever the inspection of a carrier terminal results in an unsatisfactory evaluation, the CSO, in coordination with the CSO of the HOF, will make every effort to have immediate corrective action taken. A copy of the inspection report and related correspondence will be furnished MTMC for "information only" at this point in time.

b. If immediate and effective corrective action cannot be obtained, the CSO, in coordination with the CSO of the HOF, will recommend to the Director, DIS, ATTN: Deputy Director (Industrial Security) through the Regional Director that the FCL of the terminal or the authorization for the carrier's organization to transport SECRET materials be revoked under the provisions of paragraph 2-121. Simultaneously MTMC will be requested to suspend further use of the carrier's terminal involved in shipments of SECRET materials pending decision by the Director, DIS. However, SECRET shipments already in transit may continue to be transported by the carrier to consignee.

c. Every reasonable effort will be made to have the HOF of the carrier effect required corrective action. If unsuccessful, the Director, DIS may authorize the CSO to revoke the FCL or the carrier's overall authorization to transport SECRET materials and advise the DUSD(P), ATTN: DSP&P of the action. On receipt of such notice the CSO will take the directed action and notify MTMC that the carrier (or a specific terminal) is no longer authorized to handle controlled shipments of SECRET materials.

d. If, prior to revocation, compliance with security requirements is obtained, the CSO will notify MTMC.

Part 3. "CLOSE-OUT" INSPECTIONS

4-300 A "close-out" inspection, that is, a formal DD Form 696 inspection, shall be accomplished immediately prior to action to administratively terminate a FCL or revoke a FCL. When conducting a "close-out" inspection, all areas and containers authorized for the storage of classified material shall be checked, including a spot check of other containers and areas where

classified material could reasonably be expected to be improperly stored or maintained, the latter of which shall be conducted only with the full knowledge and consent of management. Should management object to the foregoing spot-check of their non-approved areas or repositories, this fact and purported rationale shall be indicated under "Remarks" on the DD Form 696. In addition, the "Remarks" section of the DD Form 696 shall contain statements regarding: (i) the location where accountability records, records of receipt and dispatch, debriefing statements, document receipts, visitor records, destruction certificates, and so on, will be retained for the prescribed period of time, (ii) that the facility is not performing on any classified contracts, subcontracts, or proposal efforts, and (iii) *
action taken to ensure that all debriefings have been (or will be) accomplished and that outstanding classified visit authorizations have been canceled. The "close-out" inspection shall be a complete inspection *
effort, to include a listing of all deficiencies observed, inasmuch as management may justify retention of the FCL prior to completion of the termination action. A refusal by management to permit the industrial security representative to conduct a spot check of non-approved areas or repositories is not in itself significant. However, if the CSO has reason to believe that classified material remains in the facility in non-approved areas or repositories, termination of the FCL shall be held in abeyance and the matter referred to the Director, DIS, ATTN: Deputy Director (Industrial Security).

SECTION V. ESPIONAGE, SABOTAGE, LOSS, COMPROMISE, AND OTHER VIOLATIONS

5-100 Application. This section establishes the procedures for the conduct of administrative inquiries, investigations, and other administrative action required in connection with report of sabotage, espionage, and subversive activities; and the loss, compromise, suspected compromise, or security violations involving U.S. and foreign classified information (see paragraph 8-103c(4)).

5-101 Espionage, 1/ Sabotage and Subversive Activities.

a. On receipt of information from any source involving espionage, sabotage, or subversive activities not previously reported by a contractor in accordance with paragraph 6c, ISM, the CSO shall forward such information, classified if appropriate, to the nearest field office of the FBI by the most expeditious means. A copy of all referrals shall be furnished to the Regional Director and the Director, DIS, ATTN: Deputy Director (Industrial Security). The FBI will advise that office whether or not investigative jurisdiction is accepted and the CSO will be so notified. If the FBI declines investigative jurisdiction, the CSO shall initiate such other administrative inquiry or investigation of industrial security violations as may be indicated, or shall refer the case to appropriate UA's for disposition. If the FBI accepts jurisdiction, all such actions shall be deferred until completion of the FBI case. Reports of completed FBI investigations will be made available to the CSO for review, forwarding to DISCO for evaluation of any unfavorable information disclosed, and determination as to whether or not additional investigation and/or inquiry is indicated. If during subsequent actions additional information is developed which is believed to be of interest to the FBI, a report shall be furnished under the procedure outlined above for further FBI consideration.

b. On final disposition of the case by the FBI, the CSO through the Regional Director shall advise the Director, DIS and the appropriate UA(s) of all developments in the case.

1/ See paragraph 5-104 for additional reporting requirements if the espionage involves conduct which comes or appears to come within the criminal sanctions of Chapter 37, Title 18, U.S.C. 537 (reference (vv)) or of § 4 of the Subversive Activities Control Act of 1950 (Public Law 81-831, § 64 Statute 987, 989, 991, and 992, Chapter 1024) (reference (vw)).

5-102 Loss, Compromise 2/, and Suspected Compromise 3/.

a. On receipt of a report involving loss, compromise, or suspected compromise of classified information, including a preliminary report from a contractor in accordance with the requirements of paragraph 6a(2) and 7d, ISM, the CSO shall be responsible for the following.

(1) If the preliminary report indicates that other classified information may also be in danger of being compromised because of poor security practices or procedures, take immediate steps to ensure that adequate safeguards are established. This may involve an immediate visit to the facility to ensure that appropriate safeguards are established.

(2) If the preliminary report contains sufficient details to make a final determination in the case, advise the contractor in writing that no further investigation or report is required and then proceed in accordance with the procedures in paragraphs c and d below. *

(3) If the preliminary report does not contain sufficient details to reach a final determination, establish a 15-day suspense for receipt of the final report from the contractor. More time may be allotted if necessary because of the scope or complexity of the inquiry.

(4) If the preliminary report deals with foreign classified information, and the security of such information is the responsibility of the U.S., follow the procedures in paragraph 8-103c(4).

(5) If the preliminary report deals with commercial carrier CONFIDENTIAL shipments in transit, retransmit the report by electrical means within 24 hours of receipt to: Commander, Military Traffic Management Command, ATTN: MTMC-SS, Nassif Building, 5611 Columbia Pike, Falls Church, Virginia 20315.

b. On receipt of the contractor's final reports as to the results of his or her inquiry, the CSO shall accomplish the following.

(1) Review the reports for adequacy.

2/ See paragraph 5-104 for additional reporting requirements if deliberate compromise of classified information is involved; that is, any intentional act done with the object of conveying classified information to any person not officially authorized to receive it.

3/ When the facility or contractor activity is located on a UA installation, and the Commander or Head of that installation is performing certain actions on behalf of the CSO, the action which this paragraph assigns to the CSO will be performed by the Commander or Head of the installation, except for that action prescribed in paragraph 5-102d(5) which shall remain the responsibility of the CSO.

(2) Conduct additional inquiry, if necessary. Normally the contractor's inquiry shall not be duplicated except as necessary to clarify issues or to obtain additional facts. The objective is to encourage contractors to make adequate investigations and to avoid duplication of investigation. This does not negate the prerogative and responsibility of the CSO to initiate appropriate investigative action when necessary to safeguard classified information.

(3) Make a final determination that a loss, compromise, or suspected compromise did or did not occur.

c. If the final determination is made that a loss, compromise, or suspected compromise did not occur, the CSO shall ensure that the contractor has taken adequate action to prevent recurrence of such incidents.

d. If the final determination is made that a loss, compromise, or suspected compromise did occur, the CSO shall accomplish the following.

(1) Immediately furnish an advance notice with essential information to the UA contracting officers, including the ACO, so that action can be initiated to determine the extent of potential damage to the national security and to minimize the effect of the compromise or suspected compromise. The UA contracting officers should also be advised that a formal final report will follow. On receipt of the advance notification, the UA contracting officers should review the classification of the information involved for possible downgrading or declassification action. The CSO should be notified as soon as possible as to the results of the classification review and the action taken or initiated to mitigate the damage to national security. The CSO shall continue the ensuing processing without waiting for a reply from the UA contracting officer(s) if undue delay is encountered.

(2) Make a determination as to whether a weakness in security practices or procedures caused or permitted the loss, compromise, or suspected compromise, and ensure that such practices and procedures are revised to prevent recurrence.

(3) Make a determination as to whether individual responsibility can be fixed for the loss, compromise, or suspected compromise, and recommend denial or suspension of clearance, when appropriate, in accordance with paragraph 2-320.

(4) Make a determination as to the contractor's responsibility for the loss, compromise, or suspected compromise and recommend, when appropriate, action in accordance with paragraph 4-201.

(5) Make a determination in the case of lost classified material for which the contractor is unable to provide accounting as to whether the contractor's accountability for the classified item(s) should be terminated. If the circumstances of the case indicate that an adequate and exhaustive search has been made, and additional effort would not be expected to lead to the recovery of the material or provide a probable explanation of the manner of loss, the CSO shall direct the contractor to terminate accountability for the classified material in accordance with paragraph 12h, ISM. An information copy of the letter directing termination of accountability shall be forwarded

to the contracting officer concerned. If the contractor subsequently locates or recovers the classified item, a report shall be submitted to the CSO in accordance with paragraph 6a(16), ISM. Upon receipt of such report, the CSO shall notify the contracting officer concerned.

(6) Prepare a final report for record purposes. Where the investigation has been conducted by the commander or head of a UA installation in accordance with paragraph 1-108b, his or her final report will be forwarded to the CSO concerned for processing. The report will be addressed to the UA contracting officer, and a copy shall be forwarded to the ACO. A copy of the report shall be forwarded to the Director, DIS, ATTN: Deputy Director (Industrial Security) in any case where TOP SECRET information is involved. If COMSEC material is involved, a copy of the report will be furnished to the COR as required by paragraph 24 of DoD 5220.22-S-1 (reference (q)). The report, which shall enclose a copy of the final report of inquiry or a complete and detailed summary thereof, shall be prepared in the following format.

(a) Authority. Cite the reason for the inquiry including when, where, and by whom it was conducted.

(b) Essential Facts. Arrange facts (not opinions or assumptions) in chronological order. Avoid trivialities. Conflicting assertions of fact should also be discussed.

(c) Corrective Action. Specific action taken to preclude a recurrence of similar incidents and the disciplinary action, if any, taken against responsible individuals.

(d) Conclusions. Summarize conclusions reached as a result of the facts, and provide an analysis of all pertinent information bearing thereon. It is desirable, in the matter of arrangement, that the conclusions follow the sequence of the reported facts. If the conclusions of the CSO differ from a contractor's conclusions, a rationale shall be furnished.

(e) Recommendations. Include all actions required to effect disposal of the case. The recommendations shall be consistent with the conclusions. Identify those recommendations considered beyond the scope of authority of the CSO.

(f) The report shall reference the results of the review action taken by the UA contracting officer(s) with regard to downgrading or declassifying the information and mitigating the damage to national security. If the results are not known at the time of submission of the report, this fact shall be so indicated, and a copy requested when completed.

5-103 Investigative Support.

a. The CSO shall request professional investigative support from one of the three military departments when a case falls under the following criteria:

(1) any case which involves RESTRICTED DATA or FORMERLY RESTRICTED DATA, in which the CSO suspects that a criminal violation of the Atomic Energy Act of 1954 (reference (o)), as amended, has occurred; or

(2) a need exists for special investigative techniques.

b. When a case meets the above criteria, the case file together with a copy of available reports, shall be referred to the investigative agency of the military department which awarded the contract. If the contracting military department cannot be ascertained, or if more than one department is involved, the investigative agency of the military department having the principal procurement interest in the facility will assume investigative responsibility. Requests of the Office of Special Investigations, USAF (OSI) and Naval Investigative Service (NIS) investigative services shall be routed to the local field office servicing the geographical area in which the facility is located. Requests for Army investigative services shall be routed to the COMMANDER, U.S. Army Intelligence and Security Command, ATTN: LAOP-OP, Fort Meade, Maryland 20755. An information copy of such referral shall be sent to the contracting officer of the UA's concerned, the Regional Director, and the Director, DIS, ATTN: Deputy Director (Industrial Security).

5-104 Additional Reporting of Espionage, Criminal Activity, and Deliberate Compromise Cases.

a. DoD Instruction 5200.22 (reference (xx)) requires the reporting by the most expeditious means possible under the circumstances of every incident in defense industry in which espionage, criminal activity, or deliberate compromise is suspected or believed to have occurred. (Criminal activity refers to conduct that is or may be a violation of a federal or state criminal law, The Uniform Code of Military Justice, the common law, and, in addition, the criminal laws of foreign countries which might embarrass or otherwise be of concern to the DoD. Selective judgement should be exercised in determining what matters are to be reported, based on such factors as the nature of the criminal act, the clearance level of the individual concerned, and his or her relative position in the company.) When the full report required by paragraph b below would cause undue delay, an interim report containing information immediately available will be submitted.

b. When a case falls within the purview of this paragraph, the CSO, in coordination with the contractor concerned, contracting officers(s), investigative agencies, the Commander or Head of the UA installation performing security actions under the provisions of paragraph 1-108b and DISCO shall submit a report to the Director, DIS, ATTN: Deputy Director (Industrial Security) containing the following minimal information:

(1) identification of the persons involved together with a brief summary of their backgrounds including the name and address of the contractor who employs them and their PCL's -- the report shall include advice as to any action that has been taken or recommended with respect to revocation, suspension, or withdrawal of the individual's PCL;

(2) the category of classified information involved and an estimate of the time the information will retain such sensitivity;

- (3) description of the classified information involved;
- (4) evaluation of the significance to the national security of the classified information which was or might have been compromised;
- (5) summary of the circumstances of the actual or attempted compromise;
- (6) copy of any report of investigation, final or interim, conducted in connection with the compromise;
- (7) evaluation of the compromise to indicate any area of security weakness exposed by the compromise;
- (8) report of any change in the procedures of the contractor resulting from the compromise, and recommendations for any changes in the DoD Industrial Security Program that might prevent future compromises of a similar nature; and
- (9) advice as to whether disciplinary action has been taken or is recommended, or whether the incident has been referred to another federal department for appropriate further action.

c. When a case involves criminal activity, the following information shall be furnished:

- (1) full identification of persons involved to include full name, date and place of birth, local address, and present whereabouts;
- (2) facts concerning actual or attempted crime;
- (3) pending or completed action in court or other tribunal including disciplinary action taken or recommended;
- (4) a copy of any report of investigation, final or interim, conducted in connection with the crime or charge; and
- (5) a statement as to why it is believed the incident might embarrass or otherwise be of concern to the DoD.

d. On receipt of a report as described above, the Director for Industrial Security, shall review it for adequacy, resolve any inconsistencies, and transmit the report through the Director, DIS to the Director, Counterintelligence and Investigative Programs, DUSD(P), with appropriate comments.

5-105 Other Security Violations 4/.

a. On receipt of a preliminary report from a contractor in accordance with the requirements of paragraphs 6a(3) and 7d, ISM, or a report from a

4/ If this type of violation also involves the loss, compromise, or suspected compromise, the procedures in paragraph 5-102 apply.

government source, the CSO shall determine whether the circumstances involved in the violation warrant further investigation by the contractor or an administrative inquiry by the CSO, or whether the preliminary report is considered sufficient. In the latter case, advise the contractor, in writing, that no further investigation or report is required. The facts uncovered shall be evaluated and a final determination made as to what action is required by the contractor to preclude the possibility of similar violations in the future. A formal report of violations to other organizations is not required, unless the preliminary report was received from a government source. In such a case, the government source will be advised of the results of the inquiry.

b. If the violation involves classified COMSEC information (but not loss, compromise, or suspected compromise), a report shall be submitted by the CSO to the UA contracting officer and the COR as required by paragraph 24 of reference (q). A copy of the report shall be furnished to the Director, DIS, ATTN: Deputy Director (Industrial Security).

5-106 Other Administrative Violations.

e. When a report is received from a contractor, in accordance with paragraph 6a(9), ISM, that an employee refused to execute a security briefing and termination statement, the CSO shall accomplish the following.

(1) If possible, contact the former employee by letter or telephone and arrange for the former employee to execute the security termination statement and return it to the CSO.

(2) In connection with subparagraph (1) above, the CSO shall recover any classified material in the possession of the former employee.

(3) If the former employee does execute the DISCO Form 482, the form shall be forwarded to the former employer -- no further action is required.

(4) If the action taken in accordance with subparagraph (1) above is not successful, the CSO shall review the circumstances in the case. If the former employee cannot be located and circumstances suggest that the apparent disappearance may be of security significance, the FBI shall be notified. The CSO shall advise DISCO in all cases of refusal to sign the security termination statement, or whenever the former employee cannot be contacted or located. DISCO will record such information in the PSCF. If DISCO subsequently receives a request for a new PCL for the individual, the request will not be processed until the individual executes the security termination statement or provides an acceptable reason for refusal.

b. When a report is received from a contractor in accordance with paragraph 6a(10), (11), or (12), ISM, and paragraph 1-703b concerning a delay in a classified shipment, evidence of tampering with a classified shipment, or delivery of a classified shipment by unauthorized methods, the CSO will conduct additional inquiry, if appropriate, to ascertain the facts. Such inquiry could entail contact, either personal or by correspondence, with the consignor, consignee, or the carrier involved. A report of the facts, conclusions, and recommendations shall be submitted to the contracting officer and Director, DIS, ATTN: Deputy Director (Industrial Security), for review and further

action with copies to the Regional Director. If a shipment containing classified information was tampered with, advise that office what law enforcement officials were notified, if any.

5-107 Responsibility of Contracting User Agency to Investigate Certain Breaches of Security.

a. When an unauthorized public disclosure of classified information is discovered and it is not possible to determine whether it emanated from a government or industrial source, the contracting UA responsible for the information shall initiate promptly an investigation of such breach of security in order to determine the cause and establish responsibility. If a government source is involved, the contracting UA is solely responsible for ensuring adequate corrective action to prevent future compromise of this nature.

b. If the unauthorized public disclosure was from an industrial source (normally a violation of paragraph 5o, p, or q, ISM), the contracting UA will request the CSO to bring to the attention of the contractor the corrective action that should be taken to prevent future compromises of this nature.

c. If the situation warrants, the contracting UA will request the Director, DIS, to take appropriate measures against the contractor, including the revocation of the FCL in the most extreme cases. Also, the revocation or suspension of PCL's of contractor employees involved in the security breach, as provided for under the provisions of paragraph 2-320, may be recommended by the contracting UA, in which case the Director, DIS, will take the required administrative action.

d. The contracting UA will be responsible for furnishing any additional information required by DISCR, as the result of action taken in paragraph c above.

e. Action to terminate existing contracts with the facility shall be the sole responsibility of the contracting UA.

5-108 Inquiries into Delays, Tampering, or Improper Shipping Methods.

a. When, in accordance with paragraph 6a(10), ISM, the CSO is notified that a SECRET or CONFIDENTIAL shipment has not been received by the consignee within 48 hours after the expected time of arrival, the CSO shall ensure that the consignor has requested the carrier to trace the movement of the shipment and is otherwise making every reasonable effort to determine the whereabouts of the shipment. Additionally, only if the shipment was CONFIDENTIAL, the CSO shall provide a copy of the report to the Commander, MTMC, as outlined in paragraph 5-102a(5). If all efforts to locate the shipment are unproductive, the consignor shall be requested to furnish a full report of the incident, including any and all circumstances surrounding the incident. Normally the consignor shall expend no more than 72 hours to locate the shipment. The CSO shall then take appropriate action in accordance with this section.

b. When, in accordance with paragraph 6a(11) or (12), ISM, the CSO is notified of evidence of tampering with the shipment or of receipt of classified material by other than approved methods, the CSO shall conduct

appropriate inquiry only: (i) when the contractor's report of inquiry is considered inadequate, or (ii) the contractor's report is insufficient to support the contractor's conclusions that a compromise of the classified contents did or did not occur. In order to prevent a recurrence of the incident, a copy of the report received under paragraph 6a(12), ISM, shall be routed to the CSO of the contractor determined to be responsible for the violation, unless both the sending and receiving facilities are under the cognizance of the same office. If the violation was committed by a UA activity, a copy of the report shall be sent to the Commander or Head of the activity concerned.

c. The CSO shall analyze the reports required by paragraph a or b above, to determine if a particular carrier is responsible for delays in the shipment, or if a series of incidents relating to failure to comply with the shipping instructions has occurred. A record shall be maintained to identify the carrier involved. When the record shows an accumulation of reports regarding a particular carrier, the CSO shall, if the carrier is a cleared facility, conduct a comprehensive inspection of the carrier's procedures for handling a classified shipment. Recommendations for corrective action shall be submitted to the carrier if the carrier is a cleared facility, or to MTMC via the Director, DIS, ATTN: Deputy Director (Industrial Security), if the carrier is an uncleared facility. Failure of a cleared carrier to take appropriate corrective action will be considered as the basis for a recommendation for revocation of the FCL of the carrier.

SECTION VI. INDUSTRIAL SECURITY EDUCATION

6-100 Application. This section describes the educational aspects of the DoD Industrial Security Program and outlines its scope and operation. This is a two-part program designed to inform industrial management and employees of the principles of industrial security, to alert them to the dangers of espionage and sabotage, to suggest preventative measures which industry may adopt to avoid such dangers, and to acquaint the DoD and UA personnel with the principles of industrial security and with the philosophies, requirements, and techniques embodied in the DoD Industrial Security Program.

6-101 Responsibility.

a. The Deputy Director (Industrial Security), HQ DIS is responsible for the educational aspects of the DoD Industrial Security Program. This program consists of the preparation and distribution of information and technical guidance materials, and the conduct of schools for contractor and UA personnel. The scope of the education program may be expanded to include such media as the Director, DIS, or the DUSD(P), ATTN: DSP&P, considers suitable.

b. Each CSO shall be responsible for determining industrial security education and training requirements of contractors located within its geographical area, informing them of the availability of education and guidance material, and providing advice and guidance on industrial security education and training matters to contractors and indoctrination and training of UA (on request) personnel on industrial security matters.

6-102 Preparation of Material. The Deputy Director (Industrial Security), HQ DIS prepares appropriate material for dissemination in execution of this program. Suggestions from field representatives of DIS, UA's, and industry are solicited. Technical advice and assistance of the agencies of the DoD and the services of the design and art facilities of the military departments are made available for this program as requested by the Deputy Director (Industrial Security), HQ DIS.

6-103 Funding. Funds for this program shall be included in the annual budget of the DIS, including courses of instruction and field extensions of these courses, presented by the Defense Security Institute (DSI). *

6-104 Material Available. The following industrial security education and training materials shall be developed and issued by the Deputy Director (Industrial Security), HQ DIS.

a. Technical Guidance Material. Technical guidance material shall be published from time to time.

b. Wall Posters and Leaflets. Wall posters and leaflets periodically shall be developed for industrial use. Each issue will call attention to some particular phase of industrial security. The leaflets will be designed for distribution to individual employees.

c. Industrial Security Letter (ISL). The ISL shall be issued periodically to inform industry, UA's, and DoD activities of developments relating to industrial security. Local reproduction by a contractor is authorized.

d. Industrial Security Bulletin (ISB). The ISB shall be issued periodically to UA's, DoD activities, and CSO's to provide notice of current developments and pending changes within the DoD Industrial Security Program. The ISB is designed for exclusive use of the government and distribution to industry is not authorized and shall not be made.

e. Training Films. Motion picture films and strips shall be prepared for showing to industrial, UA, and DIS personnel.

6-105 Distribution of Material.

a. Technical Guidance Material. Copies of such publications, when issued, shall be furnished to UA's and/or industry (in limited quantities). Industrial facilities may purchase additional copies of designated publication directly from the Superintendent of Documents, U.S. GPO, Washington, D.C. 20402.

b. Wall Posters and Leaflets. Copies of wall posters and leaflets, when published, shall be furnished along with the ISL. Additional copies may be purchased from the Superintendent of Documents, U.S. GPO, Washington, D.C. 20402.

c. Industrial Security Letter (ISL). Industrial facilities, UA's, DoD activities, and CSO's shall be placed on the mailing list to receive limited quantities of the ISL free of charge.

d. Industrial Security Bulletin (ISB). UA's, DoD activities, and CSO's shall be placed on the mailing list to receive limited quantities of the ISB free of charge.

e. Training Films. Information concerning availability of security training films and other audio-visual aids shall be available from CSO's and the Deputy Director (Industrial Security), HQ DIS. Requests for loan of these materials may be submitted to any U.S. Army Audio-Visual Communications Center.

6-106 Training Schools. Training courses are developed, prepared, and presented under supervision and direction of Director, HQ, DIS. Program guidance is provided by the Deputy Director (Industrial Security), HQ, DIS, by the Deputy Director (Investigations), HQ, DIS, and, in the case of Information Security Management Courses and the new Basic Security (080) Course, by the DUSD(P). Courses are designed for indoctrination of contractor and UA employees and for enhancement of professional competency of DIS and UA personnel. These training courses are presented by the DSI, Defense General Supply Center, Richmond, Virginia 23297-5091 -- with periodic field extensions of courses for contractor representatives scheduled in selected areas and hosted by the CSO in the area selected. *

SECTION VII. SECURITY CLASSIFICATION AND DECLASSIFICATION7-100 Application.

a. This section prescribes the requirements and establishes the procedures to identify the classification of information turned over to contractors. It outlines the responsibility for furnishing instructions pertaining to the disposition of classified information on final delivery of goods or services or on termination of a classified contract. It also identifies other security requirements involved in prime and subcontracts.

b. This section covers the procedures to be followed by: (i) the PCO of the UA, (ii) the ACO when administration of the contract has been delegated to the DLA, (iii) the plant representative of the military department, when contract administration is delegated under the plant cognizance program this person is also referred to as the ACO, and (iv) the PCO when contract administration is retained by the PCO. Instructions pertaining to classification guidance may be issued by the PCO directly to the contractor with an information copy to the ACO or routed to the contractor through the ACO. Except for the situation covered by (iv) above, the contractor shall request guidance pertaining to classification or retention of classified information from the PCO through the ACO; however, under urgent circumstances, direct communication to obtain classification guidance is authorized with the PCO, provided that a written record of such communication is furnished the ACO.

c. In this section the term "DD Form 254" includes the "DoD Contract Security Classification Specification" (DD Form 254), attachments and supplements, as appropriate, unless specific reference is made separately to these forms in the text.

d. Security classification guidance for contractors in industry is continuously and at all times the responsibility of program, project, and systems managers, or equivalent officials (all hereinafter referred to as program/project manager), their respective successors in interest, and their respective higher level supervisors and commanders in the same channel or chain of command.

e. The complete DD Form 254, including attachments and supplements, is the basic document for conveying to contractors the applicable classification and regrading and declassification specification for a classified solicitation, contract or subcontract. It is designed to indicate, by a combination of a checklist and narrative comment, the classified areas of information involved in the classified effort and, particularly, to identify the specific items of information within these areas which require security classification protection.

f. If the classified solicitation, prime contract, subcontract, or UA program is for a research consultant service, alternate storage service, or other procurement, in which there is no requirement for a breakdown by classification of the various elements of the classified effort, the DD Form 254,

without attachments or additional guides, may be utilized for the entire contract purchase order.

g. In the absence of exceptional circumstances which clearly support classification, the DD Form 254 will not be classified. If classified supplements are required as part of the security classification specification, they shall be identified in item 15 of the DD Form 254 and be furnished as an attachment or forwarded by separate correspondence.

h. E.O. 12356 allows agency heads to waive, for good cause, the requirements for marking portions, and the preparation of classification guides for specified classes of documents or information. Exercising either of these options does not relieve a UA of the U.S. Government's responsibility, under the terms of the DD Form 441, for providing appropriate classification guidance to contractors performing on classified contracts.

i. Guidance, standards, criteria, and procedures for determining the security classification to be applied to items of information involved in a contract are provided in DoD Regulation 5200.1-R (reference (yy)) and appendix D of this regulation.

7-101 Security Classification. The DD Form 254 embodies the concept that the sensitive information itself shall be identified and assigned a proper classification rather than assigning a classification to media by which classified information could be, or would likely be, conveyed. This method of classifying information rather than media is intended to identify most precisely the functional matter which is to be protected, thus providing the answer to the question: "What is there about a specific item which causes it to be classified?" Identification and knowledge of "why" material is classified will permit greater selectivity in applying security controls, such as safeguarding, dissemination, downgrading, declassifying, and releasing. Media shall be marked as classified only if they convey information which has been identified as classified information.

7-102 Issuance of Security Classification Guidance. Program/project managers of a UA initiating procurement requests will prepare a DD Form 254 for the classified effort, and submit the specification to the UA activity PCO or his or her authorized representative for signature and necessary distribution (see paragraph 7-103). In order to increase the effectiveness of guidance furnished and provide advance notice of pending possible classification requirements, the aforementioned responsible officials should endeavor, by arrangements which are reasonable and fair to all concerned, to allow contractors and potential contractors which have the necessary FCL's the opportunity to participate in the preparation of the DD Form 254. When classified information is expected to be received or produced by the contractor, a DD Form 254 will be prepared as follows.

a. Original. Except as provided by paragraph d below, an original DD Form 254 will be issued:

(1) with each request for proposal (RFP), request for quote (RFQ), invitation for bid (IFB), or other solicitation; and

(2) with the award of a contract or follow-on contract.

b. Final. A final DD Form 254 will be issued on final delivery of goods or services or on termination of a contract provided:

(1) authority is granted under paragraph 5w, ISM, for the contractor to retain classified material originated by the UA or generated by the contractor in the performance of the contract (see paragraph 7-104); or

(2) all classified material shown in paragraph (1) above, for which retention authority would be required, is ordered immediately declassified.

(c) Revised. Revised DD Forms 254 will be issued when:

(1) at any time subsequent to the issuance of the original classification specification, additional guidance in connection with it is required to be disseminated; or

(2) at time of review, the classification specification is changed (see paragraph 7-104).

d. Special Situations.

(1) Government Furnished Equipment (GFE) or Government Furnished Property (GFP). The PCO, or his or her authorized representative, will assure that a DD Form 254 is provided for each classified item of GFE or GFP issued or authorized for purchase, after the award of contract, when such equipment or property is not covered by the guidance issued with the contract.

(2) Follow-On Contract. When item 6a identifies this as a follow-on and/or related contract, the classification guidance furnished with the DD Form 254 for the preceding contract will be identified in item 14 and be furnished as an attachment or forward under separate cover.

(3) Open-End or Call-Type Contract. A single DD Form 254 may be used to cover a basic ordering agreement or an indefinite delivery contract, except when the individual call, purchase order, or request for services or products requires classification specification different from that provided for the overall contract.

(4) Service, Graphic Arts, or Research Contracts. In these cases, a DD Form 254 is issued for every classified contract, but the scope and purpose vary.

(a) A DD Form 254 which specifies the highest level of classification involved, but does not provide detailed classification guidance, will be issued when one of the following conditions exists.

1 The total requirement of the contract is the performance of a service, all of which takes place at a cleared facility or government activity which has and makes available, for use by the contractor performing the service, a currently valid DD Form 254 which includes complete guidance for the service to be performed. In these cases, item 15 of the DD Form 254 will be annotated:

Using contractor or activity will furnish complete classification guidance for the service to be performed. The highest level of classification for the contract is (TOP SECRET, SECRET, or CONFIDENTIAL). Contract performance is restricted to (name of facility or location).

2 The contractor has no performance requirement involving actual knowledge of, generation, or production of classified information, but has only a requirement to be physically present in an area where classified information is located. Examples include, but are not limited to, contract calling for guard, alarm, alternate storage, or equipment maintenance services. In these cases, item 15 of the DD Form 254 will be annotated:

Actual knowledge of, generation, or production of classified information NOT REQUIRED. This document serves as written notice of the letting of a classified service contract. The highest level of classification for the contract is (TOP SECRET, SECRET, or CONFIDENTIAL).

3 The contract requirement is limited to graphic arts reproduction and classification markings appear on the material to be reproduced. These classification markings constitute the required security classification specification. In these cases, item 15 of the DD Form 254 will be annotated:

Reproduction service only. The highest level of classification for the contract is (TOP SECRET, SECRET, or CONFIDENTIAL). Classification markings on material to be reproduced specify the required security classification.

(b) In each of the cases described in paragraph (a) above, if a subcontract at any tier is involved, the DD Form 254 for the subcontract will not require authentication by the signature of an ACO/PCO. Instead, the contractor who is the principal prime contractor or who serves as a prime contractor in relation to a subcontractor in the particular case, will complete and sign item 16. Furthermore, in all cases, distribution of the DD Form 254 will be made to the subcontractor involved, his or her CSO, and the contract administration office(s), if designated, of the immediate prime and subcontractors involved.

(c) Where a contract involves research services requiring detailed classification guidance, but it is too early to determine these detailed requirements, item 15 of the DD Form 254 will be annotated:

This is a research contract. The highest level of classification for

the contract as a whole is (TOP SECRET, SECRET, or CONFIDENTIAL). A revised DD Form 254 will be issued as soon as possible to provide detailed security classification guidance.

(5) Commercial Carrier. By policy determination a commercial carrier does not require a DD Form 254 in connection with each transaction involving the pickup, movement, and delivery of classified material. When a cleared commercial carrier enters into a classified service subcontract with a cleared facility within the meaning of paragraph (4)(a)2 above, the carrier, serving as a prime contractor for such purpose, will issue a DD Form 254 to the cleared facility. In any such case, the requirements of paragraphs (4)(a)2 and (4)(b) above shall apply.

e. Reference Material.

(1) Original DD Form 254. In the case of a contract the performance of which is expected to require access to only reference material an original DD Form 254 will be issued to describe the highest category or various categories of classification of such material. The DD Form 254 will provide other instructions, as appropriate; for example, the protection of information extracted from such material.

(2) Final DD Form 254. A final DD Form 254 will not be issued when authority is granted under paragraph 5m, ISM, for the contractor to retain only reference material. Such material is required to be marked by its originator to reflect downgrading and declassification instructions. If it is not so marked, the contractor is responsible for requesting advice in accordance with the procedures outlined in appendix II, paragraph A5, ISM (see paragraphs 7-104 and 7-105).

f. Subcontract Guidance.

(1) Immediately on receiving notification from the prime contractor that a subcontractor has been selected and that the subcontractor is expected to require access to classified information, the ACO, or PCO if contract administration has not been delegated to an ACO, shall be responsible for the following.

(a) Ensure that the prime contractor prepares a DD Form 254 for each subcontract.

(b) Review the DD Form 254 developed by the prime contractor for each subcontract to ensure that it correctly reflects the instructions furnished by the PCO of the UA activity and is specifically designed for the particular task(s) to be performed by the subcontractor.

(c) Ensure that any questions of adequacy of the DD Form 254 are resolved to the mutual satisfaction of the prime contractor, the subcontractor and the ACO, or are referred for resolution to the program/project manager of the UA designated in item 12b on the prime contractor's DD Form 254.

(d) Except in cases falling within paragraphs d(4)(a) and d(5) above, approve the resulting DD Form 254 and make, or authorize the prime contractor to make, the required distribution. In cases falling within paragraphs d(4)(a) and d(5), the prime contractor will complete and sign item 14. Authentication by the signature of an ACO/PCO is not required.

(2) There is no authorized substitute for the DD Form 254. There are exceptional conditions in which a prime contractor has a serious time limitation in preparing his or her response to a RFP, IFB, or similar solicitation to a UA. In such cases the prime contractor, concurrent with dispatching the DD Form 254 for official government approval and signature, may supply an unofficial copy of the same guidance to a prospective subcontractor for the latter's use pending receipt and distribution of the approved and signed DD Form 254.

(3) The ACO, on receiving notification of regrading or declassification action from the PCO, shall:

(a) review the classification specification developed by the prime contractor for each subcontract which is outstanding to ensure that it correctly reflects all applicable new instructions furnished by the PCO;

(b) resolve any questions to the mutual satisfaction of the prime contractor, subcontractor, and the ACO, or refer the matter to the program/project manager of the UA designated in item 12b of the prime contractor's DD Form 254 for resolution; and

(c) approve the resulting specification, as revised if necessary, and make, or authorize the prime contractor to make, the required distribution.

g. COMSEC or Other Special Access Program Contracts. Whenever a contract requires a contractor employee to install, maintain, or operate COMSEC equipment for the U.S. Government or requires access to U.S. Government keying material, or when the contract contains other special access requirements, the contracting activity shall indicate this in item 11 of the DD Form 254. The notation should also include a statement in item 11o, "Remarks," that such COMSEC or special access information is not releasable to contractor employees who have been granted a reciprocal clearance.

h. Unsolicited Proposals. Whenever a contractor develops an unsolicited proposal or originates information not in the performance of a UA contract, the following will apply.

(1) If information is included in the proposal or other material which the contractor identifies as already being classified, the proposal or other material shall be marked with the appropriate classification by the contractor in accordance with paragraph 11, ISM.

(2) If the case does not fall under paragraph (1) above, and the contractor believes that the proposal or other material contains information which may or should be safeguarded, the contractor has been requested by paragraph 10, ISM, to protect the information as though classified at the appropriate level until an advisory classification opinion

is obtained from a UA which has an interest in the subject matter. In any such case, the protective marking to be used will be:

Classification determination pending.
Protect as though classified
(CONFIDENTIAL, SECRET, or TOP SECRET).

The marking will appear at least once conspicuously on the material, however, the contractor will not be required to mark the material further in accordance with paragraph 11, ISM, until the advisory classification opinion is received. In addition, if applicable, contractors are not precluded from designating such information as company private or proprietary information.

(a) It is the general policy of the DoD not to classify information over which it has no jurisdiction. The proposal or other material shall not be classified by the UA: (i) unless it incorporates classified information to which the contractor was given prior access or (ii) unless the government first acquires a proprietary interest.

(b) If no prior access was given, the UA shall make or obtain a determination on whether a classification would be assigned if the government held a proprietary interest. If the determination is negative, the contractor shall be advised that the information is unclassified and that the protective marking is to be removed. If the determination is affirmative, the UA shall make or obtain a determination on whether government proprietary interest will be acquired. If such an interest is acquired, the information shall be assigned a proper classification and the contractor so notified. If no such interest is acquired, the contractor shall be informed that there is no basis for classification and that the protective classification marking is to be removed.

(3) On receipt of a request for an advisory classification opinion, the activity of the UA shall:

(a) ensure that the contractor has not assigned a national security classification to the information;

(b) ensure that the material is protected as required by DoD Directive 5400.7 (reference (1)) and DoD Components' implementation thereof (see paragraph 7-108) or by equivalent requirements of UA's other than DoD; and

(c) determine whether it has an interest in the subject matter. If so, it shall take necessary action to acquire a proprietary right in the proposal or information and shall issue appropriate classification guidance. If not, it shall, when appropriate, refer the matter to another interested agency and advise the contractor of the referral. If it appears that the information or proposal is not of interest to any UA, the contractor shall be advised that a defense security classification is not warranted.

(4) Any unsolicited COMSEC system equipment, development, study, or proposal which is submitted by a contractor to a UA for consideration, shall be forwarded to the Assistant Director for Communications Security, NSA, Fort George G. Meade, Maryland, 20755, for evaluation and a

determination as to whether it requires protection in the interest of national security.

1. Public Disclosure. When a contractor reports to the ACO the appearance in the public domain of information currently classified, the ACO shall notify the PCO who shall refer the matter to the appropriate classifying authority of the UA concerned for a determination as to whether the information should be declassified, downgraded, or continued in the same classification. The contractor shall be advised promptly of this decision.

7-103 Required Distribution.

The DD Form 254, attachments, classification, and need-to-know review are to be distributed as follows 1/.

a. For Prime Contracts:

- (1) Prime contractor
- (2) CSO of prime contractor only
- (3) Appropriate ACO
- (4) Quality assurance representative
- (5) Official identified in item 12b, DD Form 254
- (6) Others as necessary

b. For Subcontracts:

- (1) Prime contractor
- (2) Appropriate ACO
- (3) Subcontractor
- (4) CSO of subcontractor only
- (5) Quality assurance representative
- (6) Official identified in item 12b, DD Form 254
- (7) Others as necessary

c. For Sub-subcontractors:

- (1) Prime contractor
- (2) Appropriate ACO
- (3) Subcontractor
- (4) Sub-subcontractor
- (5) CSO of sub-subcontractor only
- (6) Quality assurance representative
- (7) Official identified in item 12b, DD Form 254
- (8) Others as necessary

1/ Reflect the distribution in the "Required Distribution" block of the DD Form 254. For SENSITIVE COMPARTMENTED INFORMATION contracts, distribution of the DD Form 254, attachments, and supplements will be as prescribed by the procuring contracting agency concerned. Separate copies shall be furnished to the ACO, the quality assurance representative, and the CSO, so that each may discharge his or her individual responsibilities.

d. For Solicitations (IFB, RFQ, RFP). The distribution of DD Form 254 for IFB's, RFP's, or RFQ's will be the same as for the prime contract, subcontract, or sub-subcontract to which the solicitation is related, except that none is to be sent to the quality assurance representative.

7-104 Review of Classification and Need-to-Know.

a. Classification review -- except as provided in paragraph b below, the program/project manager (designated in item 12b, of the DD Form 254) of the UA activity which prepared the original, final, or revised DD Form 254 shall review the DD Form 254:

(1) during contract performance, at change of phase (such as development, order of prototype, and order of first production) or more frequently at the discretion of the PCO or his or her authorized representative, but in any event at least biennially;

(2) on final delivery of goods or services or on termination of contract, if at the time a final DD Form 254 is issued under paragraph 7-102b; and,

(3) at the conclusion of any retention period authorized under paragraph 5m, ISM, if at that time a final DD Form 254 is outstanding and the contractor requests an extension of retention authority for retained classified material which is under the classification jurisdiction of the UA. Classification review is not needed or required if the only classified material for which extension of authority is requested is reference material. See paragraph d below, for need-to-know review requirement for reference material.

b. Review of the DD Form 254 is not required:

(1) when all items of classified information were declassified or disposed of earlier;

(2) during any period for which retention authority has been granted under paragraph 5m, ISM;

(3) when the contract is classified solely because the contractor requires access to classified reference material; or

(4) when the contract is classified solely because:

(a) the contractor requires access to controlled areas containing classified information or material; or

(b) the contract is of the service type, such as for guard service or alternate storage service, where no classification breakdown of contract elements additional to that already furnished is necessary. In these cases, of course, the question of retention authority does not arise.

c. Notification -- the program/project manager (designated in item 12b of the DD Form 254) of the UA activity conducting the review shall determine whether the classified information covered by the DD Form 254 under

review shall be regraded or declassified, and require the PCO to give the prime contractor, the ACO (if any), the CSO, and other recipients of the original, final, or revised DD Form 254 written notification of the results of the review, either reaffirming the existing or issuing a revised DD Form 254.

(1) When the prime contractor receives a revised DD Form 254 providing additional guidance or a change in guidance, he or she shall prepare a revised DD Form 254 for each subcontractor whose DD Form 254 requires a related change. Authenticating signature of the ACO/PCO and distribution or instructions for distribution of the subcontractor's DD Form 254 are required.

(2) When the prime contractor receives notice that a review has affirmed his or her existing guidance, or receives a revised DD Form 254 that does not require a related change in any subcontractor's DD Form 254, the prime contractor shall promptly give written notice of reaffirmation of guidance to each subcontractor involved. This notice of reaffirmation to subcontractors does not require ACO/PCO authenticating signature, and its distribution shall be the same as for a revised DD Form 254, in accordance with paragraph 7-103.

d. Need-to-know review if extension of retention authority is requested -- if at the end of any period for which retention authority has been granted, an extension of retention authority is requested, the PCO shall conduct a need-to-know review with respect to all classified material for which an extension of retention authority is requested, including both material which is within the classification jurisdiction of such UA and reference material. If extension of retention authority is not granted, the PCO's shall require contractors to either promptly return the classified material to the PCO's or their designated representatives or destroy the classified material.

7-105 Classification Interpretation Procedures.

a. Instructions pertaining to the classification of material over which the UA has classification jurisdiction may be issued by the PCO, or his or her authorized representative, directly to the contractor with an information copy to the ACO and the CSO, or they may be routed to the contractor through the ACO. Contractors at any time may request interpretation of the classification guidance furnished them or recommended changes thereto. Except when contract administration is retained by the PCO, the contractor shall request guidance from the program/project manager listed in item 12b of the DD Form 254 through the ACO; however, under urgent circumstances direct communication with that program/project manager's office to obtain classification instruction is authorized, provided a written record of such communication is given to the ACO.

b. Classification guidance concerning reference material (see paragraph 1-254) is the responsibility of the department or agency having classification jurisdiction over such material at the time it was prepared, or of the current successor in interest of that department or agency. When contractors require classification guidance for reference material and need assistance in identifying the responsible department or agency, they shall, by direct communication, seek assistance from:

(1) the secondary distribution source from which the material was received -- examples of secondary distribution sources are the government technical information dissemination activities; DTIC, Cameron Station, Alexandria, Virginia; DoD Information Analysis Centers, and Redstone Scientific Information Center, U.S. Army Missile Command, Redstone Arsenal, Alabama;

(2) the UA contracting office last involved with the contractor concerning the subject matter of the material; or

(3) if unsuccessful in identifying the responsible department or agency by direct communication with (1) and (2) above, the contractor shall seek assistance from:

(a) the UA that awarded the prime contract, even though this will require the UA to obtain guidance from the department or agency having classification jurisdiction over such material, or

(b) the Director for Information Security, Office of the Deputy Under Secretary of Defense for Policy.

7-106 Responsibility for Authorizing Retention of Classified Material at Completion of a Contract.

a. The contractor shall request authority from the ACO (or PCO if contract administration has not been delegated to an ACO) to retain classified material on final delivery of goods or services, termination of a contract, or when a bid is not accepted. The ACO shall forward such requests for retention to the PCO. The contractor shall be granted a reasonable period of time in which to effect destruction or return of the classified material in accordance with paragraph 51, ISM, or to identify and request authority to retain that classified material for which a continued need exists.

b. The PCO, when making a determination whether to authorize retention of classified material, is encouraged to take a liberal, practical, and realistic view toward approving a contractor's request to retain classified material at the final delivery of goods or services, or when the contract is terminated for the convenience of the government. For contractors engaged in furnishing classified supplies or services on a continuing basis, the PCO should be receptive to the contractor's request when the basis for such request is to: (i) maintain an effective technical library which will be in consonance with the objectives set forth in DoD Directive 5100.36 (reference (zz)), or (ii) enable the contractor to develop future proposals for prime or subcontracts based on technologies gained in the scientific and engineering fields which have been documented and which may have a subsequent application on such proposals. The contracting officer of a current classified contract may also authorize transfer of the material to the current contract when the material is identified by the contractor in accordance with the procedures set forth in paragraph 5m(1)(d), ISM, and paragraph c below. When such approval is granted, the contracting officer who had cognizance over the classified material shall be notified by the current contracting officer. In those situations, the material shall be disposed of in accordance with paragraph 51, ISM, at the completion of the current contract. In the event that retention of information under the circumstances contemplated in this

paragraph involves information of a DoD UA being retained by a contractor of a non-DoD UA, or vice versa, or between non-DoD agencies, the concurrence of the contracting officer of the completed or terminated contract or bid which was not accepted must be obtained by the current contracting officer prior to the authorization for retention being granted. Information authorized for retention under these circumstances will be identified as to its origin, and its ultimate disposition or declassification will remain with this originating agency (see paragraph 1-110). Application of this principle will permit the contractor to have the information readily available, thereby eliminating duplication of efforts and resources, providing a savings of time which could result in reducing the cost to the government or enabling the contractor to accomplish nonsponsored research or development in a timely, efficient, and effective manner and thus be in the posture to submit proposals in connection with future government requirements. Such actions on the part of a contractor would be in the best interest of the government.

c. Authorization by the PCO to retain classified material is not required for: (i) records held by the contractor in accordance with the records retention clause of the basic contract, (ii) records authorized for retention for a specific period under the terms of the basic contract, and (iii) records which, during the contract period, the PCO has authorized the contractor to retain for a specific period following completion of the contract, provided that in each case the contractor identifies the material to be retained to the PCO in the following manner. TOP SECRET and SECRET material shall be identified in a list of specific documents. However, in the case of SECRET material only, the contracting officer may and is encouraged to authorize identification by subject matter and approximate number of documents. CONFIDENTIAL material shall be identified by subject matter and approximate number of documents. Following the completion of work under a contract or the termination of a contract where retention of classified material has been authorized by the PCO, the responsibility for follow-up actions pertaining to supplemental classification guidance and ultimate disposition of classified material reverts from the ACO to the PCO at the buying activity on both prime and subcontracts.

d. When retention of classified material is authorized by the PCO, such authorization shall prescribe a specific period of time. In reaching this decision, the PCO should be guided by the purpose for which the contractor will use this information; for example, to maintain a technical library or anticipated application to future requirements. Normally the time period authorized should be between 3 to 5 years. At the end of this period, if the contractor rejustifies his or her need for the material, the retention authorization can be renewed for additional periods.

e. When authorization to retain classified material has been granted, a review shall be accomplished in accordance with paragraph 7-104a(3). A copy of all notifications provided the contractor shall be furnished the CSO by the reviewing activity. In those cases where a subcontractor has been authorized to retain classified information at the termination or completion of a contract, the reviewing activity may make, or authorize the prime contractor to make, distribution of notices of downgrading or declassification actions.

f. On receipt of notification of the completion or termination of a classified contract the CSO, during regularly scheduled recurring security inspections, shall ensure that the contractor has complied with instructions received from the PCO and that adequate controls are maintained to safeguard the retained classified material.

g. On completion or termination, at the convenience of the government, of a classified contract involving classified intelligence information, the PCO shall require the contractor to return all classified intelligence information (furnished or generated), unless retention or destruction is authorized by the DIA or the authorized representative of the releasing UA activity.

7-107 Downgrading and Declassification.

a. Classified information or material which no longer requires its present category of protection in the interest of national security, shall be downgraded or declassified in order to preserve the effectiveness and integrity of the classification system and eliminate classification of information which no longer requires classification protection.

b. The PCO shall note on the DD Form 254, or include in attachments thereto, the declassification instructions for each element or category of information, such as a date or event for automatic declassification, or indicate that the information shall not be declassified without approval of the originating agency. If applicable, the downgrading instructions to be applied to each item of information shall be included in the classification guidance. Dates or events for declassification and, if applicable, downgrading actions shall be as soon as national security considerations permit.

c. Contractors are authorized to apply and implement provisions of the downgrading and declassification system according to the provisions of appendix II, ISM, unless otherwise instructed by the contracting activity. In those cases in which a PCO determines that the material has been improperly designated, the PCO shall instruct the contractor in writing, through the ACO, to mark the material to reflect the proper designation.

7-108 Protective Marking -- FOR OFFICIAL USE ONLY.

a. DoD Directive 5400.7 (reference (1)) does not deal with the * protection of classified information. The ISM establishes requirements for the protection of classified information. For this reason the ISM does not contain requirements for the protection of information designated "FOR OFFICIAL USE ONLY." If such information is provided to a contractor, specific notification of the requirements for protection of such information should be provided to the contractor as a separate clause in the contract, or by an official notification other than the DD Form 254.

b. Industrial security inspection services normally do not include inspection for compliance with requirements for the protection of FOR OFFICIAL USE ONLY information in possession of contractors. However, a CSO, on specific written request of the PCO, may agree to provide such inspection if resources for the accomplishment of required security inspections permit, and copies of the requirements previously furnished the contractor are provided with the request.

SECTION VIII. INTERNATIONAL SECURITY PROGRAMSPart 1. INTERNATIONAL CONTRACTS

8-100 Purpose. The purpose of this section is to set forth: the responsibilities for the protection of foreign government classified information in contracts awarded to industry within the U.S., the procedures which shall be used to ensure that the U.S. meets its obligations to protect foreign classified information, and instructions for the award of U.S. classified contracts to foreign firms.

8-101 Bilateral Security Agreements.

a. To establish the intent of both parties to protect each others classified information, the U.S. negotiates two basic types of security agreements with other governments, the General Security of Information Agreement and the Industrial Security Protocol. The Deputy Director (Industrial Security), HQ DIS is responsible for maintaining a current listing of those countries which have entered into either type of bilateral agreement. Cleared contractor facilities should contact the CSO for information concerning these agreements.

(1) The General Security of Information Agreement (GSOIA).

The GSOIA is a government-to-government agreement, negotiated through diplomatic channels. It states, in substance, that each party to the agreement will afford to the classified information provided by the other, the degree of security protection afforded it by the releasing government. It contains provisions concerning the use of each government's information, third party transfers, and proprietary rights. It specifies that transfers of information will be on a government-to-government basis. It provides that both parties agree to report any compromise, or possible compromise, of classified information furnished by the other party. Moreover, the GSOIA states that both parties will permit visits by security experts of the other party for the purpose of conducting reciprocal security surveys. The purpose of such surveys is to determine whether the foreign government has the capability to protect U.S. classified information in a manner that is substantially equivalent to the protection afforded to it by the U.S.

(2) The Industrial Security Protocol. The Industrial Security Protocol is negotiated by the DoD as an annex to the GSOIA, with those foreign governments with which DoD has entered into coproduction, codevelopment, and/or reciprocal procurement arrangements involving industry. It includes provisions for clearance of facilities and personnel, the handling and transmission of classified material, and procedures for visits.

b. The above-cited security agreements apply only when a contract, subcontract, or other such government-approved arrangement, is awarded to a foreign or U.S. contractor by, or on behalf of, the U.S. Government or the signatory foreign government, as applicable. They do not apply in the case of an industry-to-industry arrangement, unless it is

in furtherance of a documented government-to-government cooperative program, such as a coproduction memorandum of understanding. In such instances, the government-to-government arrangement will stipulate that all classified military information approved for release under the program will be safeguarded in accordance with the applicable GSOLIA and Industrial Security Protocol. If such agreements do not exist with the foreign government concerned, the necessary security provisions are incorporated in the documentation establishing the government-to-government program. Consequently, subcontracts which require the release of U.S. classified military information may be awarded to foreign industry only when: (1) the subcontract is in furtherance of a specific government-to-government arrangement or, (2) assurances are obtained through government channels that the government of the country in which the foreign industry resides will assume responsibility for ensuring the security protection of the U.S. classified information involved. All such subcontracts require the approval of the user agency having jurisdiction over the classified information involved.

8-102 General. Upon receipt of classified information furnished under the above-cited agreements, the receiving government shall administer the same security protection it applies to its own classified information of an equivalent classification level. The receiving government shall be responsible for information so received, while it is within its territorial jurisdiction or while it is possessed by, or furnished to, persons it authorized to receive such information pursuant to this arrangement. However, in the event subcontracts are awarded to a contractor in the country originally furnishing the classified information, that country will assume responsibility for the security of such information.

a. Costs. Costs incurred in conducting security investigations and inspections related to the contract will be borne by the government rendering the service. Other security costs, including the transportation of classified material, shall be borne by the party for whom the contract is to be performed. Each contract shall contain provisions concerning security costs to be incurred under the contract.

b. Transmission. Transmission of classified material shall be made only through representatives designated by each of the governments. Each contract or subcontract shall specify the transmission channels to be used. Such transmission shall be only through government-to-government channels.

c. Use of U.S. Information. U.S. contractors shall not use, incorporate, disclose, or release any U.S. classified information, other than that furnished to them for use in connection with the classified contract, without the express written authorization of the UA responsible for the information. The appropriate authority of the responsible UA shall ensure that the proposed release is consistent with the National Disclosure Policy.

d. "U.S. Munitions List" Items. If U.S. classified information or unclassified technical information on the "U.S. Munitions List" is involved in the foreign government's procurement, an export license from the Department of State is required, unless export is permitted under the

exemptions in sections 125 or 126 of the ITAR. The export authorization letter or license is prima facie evidence to the contractor that the request for disclosure of the U.S. classified information or material in the foreign government's contract has been staffed by the Department of State with the UA whose classified information is involved. However, if the license involves the release of U.S. classified information, the provisions of paragraph 65, ISM, apply.

e. Subcontracts. Unless specifically prohibited in the classified contract, the following rules apply.

(1) A U.S. contractor may subcontract within the U.S. in accordance with section VI, ISM, and within the country of the contracting government under the procedures prescribed in paragraph 8-104.

(2) A subcontract may be placed in another country only with the permission of, and under conditions agreed to by, the contracting or sponsoring government, the government of the country of the subcontractor, and the prime contractor's government.

f. Security Requirements Clause. Each government in the process of negotiating or approving a classified contract is required to incorporate in the contract document an appropriate security requirements clause, and any other security provisions of the classified contract shall be furnished to the government agency designated to furnish security supervision over the contract. The Deputy Director (Industrial Security), HQ DIS is the U.S. Government agency that shall receive security requirements clauses from the foreign government for its classified contract. In turn, the Deputy Director (Industrial Security), HQ DIS shall furnish such clause to the U.S. contractor or subcontractor through the CSO.

g. Responsibility for Channels of Transmission. The CSO will be requested by the Deputy Director (Industrial Security), HQ DIS, to designate a U.S. Government representative to serve as the channel for the transmission of classified information between the U.S. and the foreign government. The CSO will furnish guidance to the U.S. Government representative as follows.

(1) For Information to be Transmitted Outside the U.S.

(a) Ensure that the contractor has an export authorization letter or license issued by the Department of State in accordance with the ITAR (reference (1)), or that the necessary determination has been made, in accordance with the U.S. foreign disclosure policy, that the U.S. classified information or material is releasable to the foreign government concerned under a government-approved program.

(b) Ensure that the information to be exported is that for which the necessary export and disclosure authorization has been obtained and does not contain other U.S. classified information in the possession of the contractor, unless specifically authorized in writing as prescribed in paragraph 8-102c above.

(c) Verify that U.S. classified material authorized for release to the foreign government is marked with the U.S. classification and the equivalent foreign classification. Affix the foreign country name before its classification marking, and type "U.S." before the U.S. classification. If the equivalent foreign classification is in English, an additional classification marking is not necessary. The U.S. classified material authorized for release to the foreign government will bear an appropriate downgrading and declassification marking.

(d) Examine the material for proper packaging in accordance with paragraph 17, ISM.

(e) Obtain instructions on how and where to ship from the Deputy Director (Industrial Security), HQ DIS, through the CSO, after such instructions have been obtained from the foreign government representing the foreign procuring activity. The method of shipping will be in accordance with UA shipping regulations or instructions while the material is under U.S. control, before delivery to the foreign procuring activity.

(f) Obtain an appropriate receipt for the shipment from the representative of the foreign government.

(2) For Information Received from Outside the U.S.

(a) If the foreign classification is not in English, affix the equivalent U.S. classification marking to the foreign classified material, note the foreign country name before its classification marking, and mark "U.S." before the U.S. classification (see paragraph 11e, ISM). If the foreign classification appears in English, an additional classification marking is not required. *

(b) Forward to the contractor, in accordance with U.S. rules for safeguarding classified information, the classified information received from the foreign government or its representatives. When requested by the foreign government, ensure that the contractor furnishes receipts for the information.

(c) Maintain a record of receipt and dispatch of all foreign classified material.

8-103. Foreign Government Classified Contracts or Subcontracts to U.S. Industry.

a. The procedures of this section apply to the protection of foreign government classified information released to a cleared U.S. contractor. They apply to those cases in which contracts, subcontracts, or precontract negotiations, involving foreign classified information, hereinafter referred to as classified contracts, are placed or entered into within the U.S. by a foreign government or a foreign firm on behalf of the foreign government. Normally, a foreign government will place a classified contract through U.S. Government channels. The initial point of contact on the

placement of a foreign classified contract in the U.S. will be the Deputy Director (Industrial Security), HQ DIS. If the CSO ascertains, either through the U.S. contractor concerned or by recurring inspection, that a foreign classified contract has been placed outside government channels, such information shall be reported immediately to the Director, DIS, ATTN: Deputy Director (Industrial Security). That office, after contacting the foreign government concerned, will furnish to the CSO appropriate instructions for handling the security aspects of the foreign contract. The CSO will ensure that appropriate instructions are provided to the U.S. contractor concerned.

(1) Expect as provided in paragraph (2) below, the Deputy Director (Industrial Security), HQ DIS will administer the security aspects of such contracts including establishment of channels of transmission of classified information or material.

(2) A UA may administer the security aspects of classified contracts including the establishment of channels of transmission of classified material or information in the following cases:

(a) for contracts in support of the Mutual Aid Program (MAP),

(b) when the U.S. Government, through a UA, contracts for classified defense material, including technical data, for delivery to a foreign government, and

(c) when the UA is designated as the executive agent ^{1/} to monitor a classified contract awarded to a U.S. contractor by a foreign government.

b. When the Deputy Director (Industrial Security), HQ DIS, determines that an appropriate security agreement does not exist, it will so advise the CSO. In the absence of a specific security agreement or other type of agreement containing a security clause obligating the U.S. Government to protect the foreign government's classified information, the contractor will be advised by the CSO to that effect, that the U.S. Government does not ensure the safeguarding of any foreign classified information released directly to the U.S. contractor, and that such information will be protected in accordance with instructions received from the foreign government or foreign contractor releasing the information to the U.S. contractor. The U.S. contractor shall be advised by his or her CSO that when an appropriate security agreement does not exist, the contractor shall not indicate or infer that the U.S. Government will be involved in the safeguarding of any foreign classified information released to the U.S. contractor. The contractor should notify the foreign government involved.

^{1/} The executive agent is the UA appointed by appropriate authority within the DoD to act for a foreign government in that foreign government's contract with U.S. industry.

c. Responsibilities of the Deputy Director (Industrial Security), HQ DIS.

(1) Effect necessary coordination of security matters between activities of the DoD and UA's.

(2) Establish, subject to the provisions of this and other applicable regulations, procedures for the transmission of classified information between the foreign country and the U.S., and the U.S. and the foreign country. These procedures will be coordinated with the designated agency of the foreign government which is responsible for security measures related to the contract. Appropriate guidance shall be furnished to the CSO (see paragraph 8-102g above).

(3) Notify the contractor, through the CSO, of the procedures for the transmission of classified information which have been established.

(4) Notify the CSO when the precontract discussion between the foreign government and the U.S. facility on the contract being performed will involve the release or disclosure of foreign classified information to a facility.

(5) Obtain security classification guidance from the foreign government, assign equivalent U.S. security classification, and furnish copies of it to the contractor through the CSO.

(6) Assist the contractor in resolving questions concerning classification of foreign government information. In coordination with the designated foreign government agency, arrange for a review of the foreign classified information for downgrading or declassification during performance of the contract and when the contract is completed.

(7) Obtain copies of the security requirements clause and any other security provisions of the contract. Forward copies to the CSO and the contractor, through the CSO.

(8) Coordinate with the ACO to ascertain that the actions set forth in the table in paragraph e below, which the ISM and this regulation charge to the ACO, have been taken. Coordinate with the designated agency of the foreign government prior to taking any action hereunder which will result in a direct security cost, or when otherwise necessary. (Duties not specifically assigned herein are reserved to the foreign government or foreign contracting activity concerned.)

(9) On receipt of report from the CSO under paragraph c(4) below, advise the foreign government concerned.

d. Responsibilities of the CSO. The CSO shall perform the functions prescribed in the ISM and this regulation on the same basis as would apply to a facility performing on a U.S. classified contract. This shall include, but shall not be limited to, the granting of a FCL required to

accomplish the foreign classified contract, the conduct of FCL surveys, and the performance of industrial security inspections. In addition, the CSO shall be responsible for the following.

(1) Take the action set forth in the following table which the ISM and this regulation charge to the CSO.

(2) Submit through the Director, DIS, ATTN: Deputy Director (Industrial Security), to the ACO for approval, any action hereunder which will result in a direct security cost, or when otherwise necessary.

(3) Ensure that contractors having access to foreign classified information are informed of their responsibility to safeguard it in accordance with applicable laws, regulations, and security agreements.

(4) Report promptly to the Director, DIS, ATTN: Deputy Director (Industrial Security), by phone or message, the loss, compromise, or suspected compromise of foreign classified information, which occurs while the security of the information is a responsibility of the U.S. This advance notice should include a brief statement of the facts surrounding the incident and an indication as to when the complete investigative report will be submitted. Under no circumstances should the CSO communicate directly with agencies of the foreign governments on such matters.

(5) Report to the Director, DIS, ATTN: Deputy Director (Industrial Security), when in the course of recurring inspections or by other means, it is ascertained that a foreign classified contract has been placed by either a foreign government or a foreign contractor with the U.S. contractor (without having utilized secure government-to-government channels).

(6) Mark the U.S. classified material, or cause it to be marked, with the equivalent foreign security classification.

(7) Examine classified material, or cause the material to be examined, which is proposed for transmission to the foreign government or its representatives, to ensure that only authorized U.S. classified information is contained in the shipment.

(8) Ensure that the shipment, to the point where the representative of the foreign government accepts security responsibility, is made in accordance with U.S. regulations for the transmission of classified information.

(9) Obtain an appropriate receipt for the shipment from the representative of the foreign government.

(10) Include a provision in the contract that all U.S. classified information furnished or generated under the contract with the foreign government or contractor shall be returned on completion or termination of the contract to the UA of the U.S. contractor, in the case of a subcontract, or that permission to retain the information shall be obtained from the UA.

(11) The UA shall inform the Director, DIS, ATTN: Deputy Director (Industrial Security), when it authorizes a U.S. contractor to place a U.S. classified contract in a foreign country involving disclosure of U.S. classified information to the foreign country.

e. Table of Functional Responsibilities - Foreign Classified Contracts. Certain duties which this Regulation and the ISM assign to the contracting officer or to the contracting User Agency are, with respect to foreign classified contracts, assigned to the Deputy Director (Industrial Security), HQ DIS, the administrative contracting officer, or the cognizant security office. Table 1 shows the assignment of these responsibilities. Duties not specifically assigned in the table are reserved to the foreign government agency or foreign contracting activity concerned (see paragraph 1-10ld(2)). Requests for instructions concerning security responsibilities reserved to the foreign government or foreign contracting agency shall be submitted through the Director, DIS, ATTN: Deputy Director (Industrial Security).

*
*
*
*
*
*
*
*
*
*
*

Table 1

| Action | References | Deputy Director (Industrial Security), HQ DIS | | | ACO | CSO |
|---|----------------------------|--|---|--|-------|-----|
| | | | | | | |
| 1. Approves retention of classified information by contractor or subcontractor. | Pars. 51 5m and 64, ISM | ----- | | | x | |
| 2. Authorizes and provides instruction for transmission of classified information outside the facility. | Pars. 5 and 17, ISM | ----- | | | x | x |
| 3. Authorizes reproduction of classified information. | Par. 18, ISM | ----- | | | x | |
| 4. Authorizes destruction of certain classified information. | Par. 19, ISM | ----- | | | x | |
| 5. Approves visits for Categories 2 and 3 visitors. | Par. 41, ISM | ----- | | | x2/ | x |
| 6. Approves electrical alarm service. | Pars. 35 and 36, ISM | ----- | | | x3/ | x |
| 7. Approves controlled areas. | Par. 34, ISM | ----- | | | x3/ | x |
| 8. Authorizes disclosure of TOP SECRET (TS) information to subcontractor. | Par. 59, ISM | ----- | | | x | |
| 9. Receives notification of award of classification subcontract 4/. | Par. 62, ISM | | x | | x | x |
| 10. a. Approves security classification guidance for subcontracts. b. Obtains security classification guidance for subcontracts. | Par. 60, ISM | ----- | | | x | |
| 11. Investigates security violations. | Section 5, ISR | ----- | | | ----- | x |
| 12. Takes action regarding certain interim PCL's and PCL's 5/, if there will be a crucial delay in the contract performance. | Pars. 2-102 and 2-307, ISR | | x | | ----- | x |

2/ Some foreign contracts will be managed by the country's personnel directly from the country concerned, its Washington embassy, or other means with no U.S. contracting officer involved. U.S. UA's control Category 4 visits as well as Category 3. Necessary coordination will be effected with the Deputy Director (Industrial Security), HQ DIS, the CSO, and the contractor concerned.

3/ If costs are involved, the ACO authorizes reproduction of classified information.

4/ This notice shall be sent to the CSO of the subcontractor.

5/ Approval on interim PCL's will be taken by DISCO at the direction of the Deputy Director (Industrial Security), HQ DIS.

8-104 Procedure for the Security of U.S. Classified Contracts or *
Subcontracts Awarded to a Foreign Contractor. *
The UA may initiate action *
to award, or permit one of its contractors to award, a classified contract *
to a foreign contractor in accordance with the UA regulations, provided the *
classified information involved has been approved for release (or is deter- *
mined to be releasable) to the government of that country under the National *
Disclosure Policy, and the foreign government concerned has entered into a *
security agreement or other security arrangement with the U.S., under which *
it agrees to protect U.S. classified information released to it (see para- *
graph 65, ISM, and 8-101). *

a. The UA acting on its own behalf, or on behalf of its con- *
tractors or subcontractors, shall communicate directly with the designated *
foreign agency to accomplish the following. *

(1) Request approval for the placement of prime contracts or *
subcontracts in the foreign country. *

(2) Obtain the necessary security assurance or arrange for *
the clearance of the foreign facility to be visited and approval of visits *
of U.S. personnel necessary to carry on precontract negotiations leading to *
the award of a classified contract. *

(3) Request approval for individual visits, or establish an *
approved list for continuing visits, to activities in the foreign country in *
connection with the classified contract. Requests for approval of visits *
shall include the information set forth in paragraph 37d, ISM. The general *
policies relating to visits set forth in paragraph 3-400 are equally appli- *
cable to visits in connection with U.S. contracts awarded to firms in for- *
eign countries. *

b. On approval of the contract by the foreign government, the *
UA shall be responsible for the following. *

(1) Include, or cause to be included, a security require- *
ments clause in each U.S. classified contract awarded to a foreign firm. *
This shall include any special security requirements necessitated by *
differences in the industrial security system of the foreign government. *

(2) Specify in the security clause, limitations, if any, *
to be placed on the authority of the contractor to place classified *
subcontracts. *

(3) Furnish, to the designated foreign government agency *
security classification guidance for each classified contract. Guidance *
shall be kept current and reviewed for downgrading or declassification *
action when the contract is completed. *

(4) Establish, subject to the provisions of this and other *
applicable regulations, procedures for the transmission of classified infor- *
mation between activities in the foreign country and activities in the U.S. *
These procedures shall be coordinated with the CSO and the designated agency *
of the foreign government. *

(5) Designate the U.S. activity or representatives through which all transmission of classified information between the U.S. and foreign government shall pass. *

(6) Mark the U.S. classified material, or cause it to be marked, with the equivalent foreign security classification. *

(7) Examine classified material, or cause it to be examined, which is proposed for transmission to the foreign government or its representatives, to ensure that only authorized U.S. classified information is contained in the shipment. *

(8) Ensure that the shipment, to the point where the representative of the foreign government accepts security responsibility, is made in accordance with U.S. regulations for the transmission of classified information. *

(9) Obtain an appropriate receipt for the shipment from the representative of the foreign government. *

(10) Include a provision in the stating contract that all U.S. classified information furnished or generated under the contract with the foreign government or contractor shall be returned on completion or termination of the contract to the UA or U.S. contractor, in the case of a subcontract, or that permission to retain the information shall be obtained from the UA. *

c. The UA shall inform the Director, DIS, ATTN: Deputy Director (Industrial Security), when it authorizes a U.S. contractor to place a U.S. classified contract in a foreign country involving disclosure of U.S. classified information to the foreign country. *

Part 2. PROCEDURES PERTAINING TO U.S. PATENT AGENTS ENGAGED IN FILING CLASSIFIED PATENT APPLICATIONS FOR FOREIGN GOVERNMENTS *

8-200 Application. *

a. In order to conform with agreements entered into between the U.S. Government and certain foreign governments pertaining to the reciprocal filing of classified patent applications, the following procedures have been developed by the DoD and the representatives of certain foreign governments. *

b. These procedures will apply only to those cases in which U.S. patent agents are engaged in filing classified patent applications in the U.S. Patent Office under a secrecy order on behalf of one of the participating foreign governments (see paragraph 8-203). *

c. The DoD industrial security procedures shall be used to protect the foreign classified information released to U.S. patent firms. *

8-201 General. The DIS, on the request of the designated representative of the participating foreign government, will assume responsibility for the FCL of U.S. patent firms that will be engaged in this program. *

a. The foreign government concerned will request the Armed Services Patent Advisory Board (hereinafter referred to as the Board) to provide information as to the clearance status of U.S. patent firms prior to the release of any classified information to the firm. *

b. The Board will forward the request to the Director, DIS, ATTN: Deputy Director (Industrial Security). *

c. If the firm either does not possess a FCL or the current clearance is at a lesser level than required, the CSO will be requested by the Deputy Director (Industrial Security), HQ DIS to process the firm for an appropriate FCL. On completion of such action, the Deputy Director (Industrial Security), HQ DIS will be advised. In turn, HQ DIS will notify the Board. *

d. The Board will inform the foreign government concerned of the status of the clearance and the address of the CSO which has security cognizance over the facility. *

e. After a clearance has been granted or confirmed, the foreign government concerned may then deliver the classified information to the facility, or it may send the classified information through the CSO. At the discretion of the foreign government concerned, the U.S. patent agent may be authorized to return the foreign government's classified information directly to that foreign government. On the initial release of the information to the facility, the foreign government concerned will notify the CSO that the classified material has been physically delivered and specify the channel for transmission of foreign classified information which the U.S. patent agent has been authorized to follow. *

f. On receipt of such notice, the CSO will inform the facility that it is obligated to protect the classified information furnished to it in accordance with the procedures established in ISM. *

g. If the foreign government concerned is advised by the Board that the U.S. patent agent does not have the capability to physically safeguard the classified information, the foreign government may transmit the classified information to the designated CSO. In such cases, the CSO shall retain physical custody of the classified information, until the facility develops the necessary capability for safeguarding. The classified information shall then be delivered to the facility by the CSO. The CSO shall advise the Director, DIS, ATTN: Deputy Director (Industrial Security) when the facility develops the ability for safeguarding and when the classified information has been delivered. That office shall then inform the Board. The Board, in turn, shall notify the foreign government. *

h. So long as a foreign government or firm maintains an agreement or contract with a cleared patent attorney or agent in the U.S. for the filing of classified foreign patents, the CSO shall keep the Deputy Director (Industrial Security), HQ DIS informed of any change in the status of the facility. *

i. If the foreign government concerned desires to release information of a higher classification category than the level of the FCL, the foreign government will request information from the Board regarding the eligibility of the facility to receive the higher category of classified information.

j. The above procedures shall not apply when TOP SECRET information is involved. If a requirement should arise involving a patent application in the TOP SECRET category, the matter will be handled on an individual basis between the foreign government concerned, the Board, and the Deputy Director (Industrial Security), HQ DIS. The Deputy Director (Industrial Security), HQ DIS shall determine the security requirements in the specific case and shall so advise the CSO.

8-203 Participating Countries. The following countries have executed agreements to participate in this procedure: Australia, Belgium, Canada, Denmark, Republic of France, Federal Republic of Germany, Greece, Italy, Luxembourg, The Netherlands, Norway, Portugal, Sweden, Turkey, and the U.K.

Part 3. OFFICE OF INDUSTRIAL SECURITY INTERNATIONAL

8-300 General. The DoD has established the OISI to provide administrative assistance for industrial security purposes to U.S. industry in their marketing, liaison, and technical assistance activities outside the U.S. The OISI operates under the supervision and direction of the Deputy Director (Industrial Security), HQ DIS. The OISI acts as the central file outside the U.S. for information pertaining to security clearances and security assurances for U.S. citizen contractor employees assigned outside the U.S. Such information from the file is available for official use by agencies and activities of the U.S. Government, foreign governments, NATO, and U.S. contractors.

8-301 Functions.

a. The OISI assists U.S. industry, foreign governments, and international pact organizations by processing classified visit requests for U.S. contractor employees, and by providing: storage for classified material; secure mail channels for transmission of classified material between a contractor in the U.S. and an approved destination outside the U.S., when specifically authorized by the Deputy Director (Industrial Security), HQ DIS; and security briefings, orientations, and certificates.

b. When assigned, the OISI inspects contractor activities on U.S. Government installations outside the U.S.

8-302 Addresses.

a. Military Mailing Address — Office of Industrial Security International, APO New York 09667

b. Civilian Mailing Address — Office of Industrial Security, International, Steenweg Op Leuven 13, 1940 St. Stevens-Woluwe, Brussels, Belgium

*
*
*

c. U.S. Cable Telegram Address — OISI Brussels, Belgium

*

d. Other Cable -- OISI, American Embassy, Brussels, Belgium, 1000 Brussels, Belgium

e. TELEX Address -- OISI, American Embassy, 21336, Brussels

f. Telephone -- Brussels 0-322 720-8259

g. Mannheim, West Germany, Field Office -- Commercial
(49621) 472582, Autovon 380-8363

h. OISI - Far East (FE), Yokohama, Japan -- Commercial
045-441-0378, Autovon 235-6703

*
*
*
*

Part 4. OVERSEAS OPERATIONS OF U.S. CONTRACTORS

8-400 General.

a. This part sets forth access and safeguarding requirements for cleared U.S. citizen employees of U.S. contractors assigned to duty stations outside the U.S. These requirements also apply to U.S. citizens who, in addition to being cleared as employees of cleared U.S. contractors, also are dual-status employees of foreign subsidiaries which are wholly owned and controlled by cleared U.S. facilities.

b. This part does not apply to:

(1) uncleared employees of cleared U.S. contractors who are stationed outside the U.S.,

(2) U.S. citizens who are representatives of any foreign interest or employees of foreign subsidiaries of cleared U.S. facilities but do not hold dual-status employment with the owning or controlling U.S. facility, and

(3) representatives (not employees) of cleared U.S. contractors.

c. Cleared employees of U.S. contractors stationed overseas are eligible to attend periodically scheduled security briefings conducted by the OISI. These briefings are designed to familiarize the employee with the international aspects of the DoD Industrial Security Program and the security requirements unique to the foreign countries in which the contractor does business.

8-401 Access. Contractors are authorized to grant access to U.S. classified information to their cleared employees who are assigned overseas, subject to the following.

a. Access to U.S. classified information identified in this sentence shall be granted only with the prior written approval of the UA having primary interest in the information concerned:

(1) TOP SECRET information,

(2) RESTRICTED DATA OR FORMERLY RESTRICTED DATA,

(3) COMSEC and COMMUNICATIONS ANALYSIS information (see paragraph 6 of reference (q)),

(4) special access programs information (see paragraph 5, ISM), and

(5) information for which foreign dissemination has been prohibited in whole or in part.

b. Access shall be limited strictly to that information required by employees for performance of the specific duties or contracts for which they are assigned overseas. Furthermore, access to U.S. classified information under this part shall be made, to the maximum extent practical, on an oral or visual basis. When physical access is to be granted to an employee, the appropriate safeguarding provisions set forth in paragraph 8-402, shall be strictly complied with.

c. Access to U.S. classified information for cleared employees assigned overseas may be granted both in the U.S. and overseas.

d. Access to U.S. classified information granted to cleared employees of a cleared U.S. facility who are also employees of a U.S. wholly-owned and controlled foreign subsidiary of such facility is granted only in their capacity as employees of the cleared U.S. facility. Contractors granting the access are responsible for ensuring that their employees provide the required safeguards for any classified information which may be disclosed to them. In addition, contractors shall take appropriate action to ensure that U.S. classified information entrusted to the employees is not further released or made available to other employees of the foreign subsidiary.

8-402 Safeguarding U.S. Classified Information. The following additional safeguards are prescribed in connection with U.S. contractor overseas operations.

a. Transmission. Transmission of classified material outside the U.S. by cleared contractors shall be in accordance with paragraph 17e, ISM. Hand-carrying of classified information by cleared contractor employees is not permitted, unless it is accomplished in accordance with paragraph 1-602e(1). The material must be addressed to a U.S. military activity or other U.S. Government activity, and must be marked for the attention of the contractor or the employee for who it is intended. The U.S. activity will notify the contractor or contractor employee of the receipt of the material. Classified material must be transmitted only through U.S. Government channels. Normally transmission will be by Registered Mail through U.S. Military Postal Service or by ARFCOS. However, the contracting officer may authorize any of the other approved methods of transmission described in paragraph 17e, ISM. If disclosure authorization is required and has been obtained, it should be cited in the transmission document with the effective dates and any other limitations. The contractor must make prior arrangements for the storage of U.S. classified material with a U.S. military installation, the OISI, a military attache, a MAAG and Office of Defense Cooperation or a U.S. diplomatic or consular office, prior to transmitting U.S. classified material overseas.

b. Custody and Storage.

(1) Personnel authorized access to U.S. classified material overseas will normally only be permitted such access at a U.S. Government activity. The storage of U.S. classified material overseas at any location other than a U.S. Government-controlled installation is prohibited.

(2) It is the responsibility of the U.S. Government representative acting as custodian for the classified material to ensure him or herself that: (i) the contractor employee has an appropriate security clearance for the level of access involved, (ii) an established need-to-know, and (iii) that the presence of classified material overseas has been authorized by the contracting officer. Additionally, the U.S. Government activity providing storage for the contractor shall establish procedures to ensure that classified material removed from storage for use is either returned at the end of the workday or is to be stored at another U.S. military or U.S. Government-controlled installation.

(3) Classified material which is in temporary storage for contractors is the responsibility of the holding activity and is to be handled and stored in accordance with regulations applicable to the host activity. The material shall not be controlled in any more lenient manner than the host activity's own classified material.

(4) If, in the performance of a contract, project, or mission unusual conditions make it necessary for a contractor employee to have temporary physical custody of U.S. classified material, authorization for removal must be obtained from a responsible official of the holding activity. When such custody is authorized, the employee is responsible for personal possession and surveillance of the material. Immediately following the purpose for which the material was needed and the removal was authorized, but in all cases prior to the end of the workday, the material is to be returned to the U.S. Government activity for storage purposes. While in transit in the employee's custody, the classified material must be double wrapped and accompanied by either: (i) a contractor employee, courier, or escort who is cleared for access to the level of the classified information involved, or (ii) accompanied by a U.S. Government civil service employee or military person who is cleared for access to the level of the classified information involved. Hand-carrying of classified material by contractor employees across international boundaries is prohibited. In the event the contractor has not returned the classified material at the end of the workday and arrangement for approved storage elsewhere has not been made, the U.S. Government representative shall immediately initiate an inquiry to determine all the facts. If appropriate, a spot report will be forwarded to DISCO and the CSO of the HOF with information copies to OISI, the Deputy Director (Industrial Security), HQ DIS, and the contracting officer. Subsequently, a complete report will be made and submitted to the same addresses. The CSO will bring the matter to the attention of the contractor's HOF and obtain an assurance from the management that there will be no recurrence. DISCO, on receipt of the report, will, if appropriate, take the action required by paragraph 2-230. The CSO and DISCO will advise the government activity initiating the inquiry, and the contracting officer, of the results of the action taken.

c. Disclosure. Except as provided for in paragraph 3-400, contractor personnel are not authorized to disclose classified information to any foreign government or its representatives. Cleared contractor personnel overseas may, however, disclose classified information:

(1) to other cleared personnel within their company who have been granted a LOC at the required level and who have a need-to-know for access to the information concerned,

(2) to any appropriately cleared military or civilian member of a UA who has a valid need-to-know, and

(3) outside the contractor's organization within the U.S. only in accordance with the ISM, and outside the U.S. only in accordance with specific instructions from the contracting officer of the UA.

Part 5. ACCESS TO CLASSIFIED INFORMATION OF FOREIGN GOVERNMENTS AND INTERNATIONAL PACT ORGANIZATIONS UNDER A U.S. SECURITY ASSURANCE

8-500 General. In its relations with friendly and allied foreign governments, the U.S. has entered into various treaties and agreements whereby each signatory government agrees to safeguard the classified information released to it by the other government. These range from bilateral agreements which provide only that each government will safeguard, in accordance with mutually agreed procedures, the classified information released to it by the other government, and that the information will not be disclosed to a third country without the consent of the originating government, to multilateral treaties establishing international organizations for concerted defense, with either a technical annex establishing the detailed procedures and standards for safeguarding classified information originated or disseminated by the organization, or provisions authorizing the organization to establish mutually agreeable regulations for safeguarding such information.

8-501 Security Assurances.

a. In order to assist U.S. cleared contractors in meeting personnel security requirements imposed by friendly and allied foreign governments with whom the U.S. has entered into bilateral security agreements for access by U.S. citizens to foreign classified material, which is under the contract of the foreign government or organization, the contractor will send a request for the necessary security assurance to the Director, DISCO. The application shall be made in accordance without the requirements of paragraph 99a, ISM.

b. DISCO shall ascertain the security status of the individual and make a security assurance determination. A favorable determination will result in issuance of the security assurance to the requesting contractor; a DISCO Form 560 will also be entered into DISCO's files, but will not be issued to the contractor unless, in accordance with paragraph 99a(3)(e), ISM, access will include U.S. originated and appropriately marked classified information. This action will involve making inquiry of the PSCF, a UA, or other federal agency, according to available information regarding clearance

status of the individual. If the individual does not have a valid LOC on file, DISCO shall initiate an appropriate investigation. If the security assurance requested is for SECRET or CONFIDENTIAL, a NAC is required. If the assurance requested is for TOP SECRET, a BI is required. If DISCO can not make a favorable determination, or there is a justifiable need to suspend or revoke a LOC on which the security assurance has been issued, DISCO will follow the procedures in paragraph 2-320.

8-502 Administrative Termination of Letters of Consent. On receipt of notification from the contractor under paragraph 6b(b), ISM, that a cleared immigrant alien resides or is assigned outside the U.S., Puerto Rico, Guam, or the Virgin Islands, DISCO will administratively terminate without prejudice the LOC issued the individual and so advise the contractor.

8-503 Annotation of Clearance Records. On receipt of the report of an overseas assignment required by paragraph 6b(2), ISM, DISCO will annotate the PSCF to reflect the employee's new duty assignment and notify OISI of the action, so that OISI may amend its records. The PSCF, and the record provided to OISI, shall reflect that the briefing prescribed by paragraphs 97 and 99a, ISM, has been accomplished.

SECTION IX. INDUSTRIAL SECURITY FORMS**Part 1. GENERAL**

9-100 **Application and Index of Forms.** The purpose of this part is to list and explain the purpose of forms prescribed for use in the DoD Industrial Security Program. Six of the listed forms (DD Forms 374, 555, and 696; DIS Forms 553 and 1148) are exhibited in part 2. All other listed forms are exhibited in the ISM or supplements thereto. These forms shall not be used for any purpose or in any other manner except as provided for in this regulation or for training purposes.

a. **DD Form 48.** "Department of Defense Personnel Security Questionnaire (Industrial-NAC)" -- this form is used to obtain SECRET clearances for employees who are U.S. citizens.

b. **DD Form 48-2.** "Application and Authorization for Access to CONFIDENTIAL Information (Industrial)" -- this form is utilized by contractors to obtain the data necessary as the basis for granting a CONFIDENTIAL clearance to a U.S. citizen employee.

c. **DD Form 48-3.** "Department of Defense Personnel Security Questionnaire (Updating)" -- this form is used to obtain current and updating personal data needed to process a clearance action when an individual with a PCL is transferring employment from one contractor to another contractor within a 12-month period and requires a PCL in his or her new employment. It also is used in converting a UA clearance to an industrial PCL.

d. **DD Form 49.** "Department of Defense Personnel Security Questionnaire (Industrial)" -- this form shall be used in making application for:

- (1) a U.S. citizen being considered for a TOP SECRET PCL,
- (2) a U.S. citizen being considered for any level of clearance when the individual advises he or she is a representative of a foreign interest,
- (3) a U.S. citizen who has relatives or relatives of his or her spouse who are residing in Communist countries,
- (4) an immigrant alien being considered for a PCL, and
- (5) a citizen of a country with which the U.S. has entered into a reciprocal agreement who is being processed for a reciprocal clearance.

e. **DD Form 254.** "DoD Contract Security Classification Specification" -- this form, including attachments and supplements, as applicable, is the basic document by which classification, regrading, and declassification specifications are documented and provided to prime and subcontractors.

f. FD Form 258. "Applicant Fingerprint Card" -- this form is completed for all personnel being considered for a PCL, an overseas security eligibility determination, or a reciprocal clearance.

g. DOE Form F 5631.20. "Request for Visit or Access Approval" -- this form is listed for information purposes. It is used for processing visits involving access to RESTRICTED DATA. Copies of this form may be obtained from the DOE.

h. DD Form 374. "Facility Security Clearance Survey" -- this survey form is completed by the CSO as a prerequisite to granting a FCL.

i. DIS FL 381-R. "Letter of Notification of Facility Clearance" -- this letter is prescribed for use by a CSO to notify a facility that it has been granted a FCL.

j. DD Form 441. "Department of Defense Security Agreement" -- this form is prescribed for use by the CSO in obtaining the formal agreement of management of a facility to abide by the DoD LSM (attachment to DD Form 441).

k. DD Form 441-1. "Appendage to Department of Defense Security Agreement" -- the DD Form 441-1 is used when management desires to indicate multiple facility coverage with one "Department of Defense Security Agreement." After a DD Form 441 has been properly executed, a contractor may use the DD Form 441-1 to accomplish additions, deletions, or changes in the branches or facilities included in and covered by the original DD Form 441.

l. DD Form 441s. "Certificate Pertaining to Foreign Interests" -- this form is prescribed for use by the CSO in obtaining a formal certification from the contractor relative to FOCI.

m. DISCO Form 482. "Security Briefing and Termination Statements (Industrial Personnel)" -- this is a two-part form prescribed for use by employees of contractors. Part I shall be executed by employees following their initial security briefings and prior to being granted access to classified information. Part II shall be executed by employees during their termination proceedings.

n. DIS Form 553. "Central Index File Card-Facility" -- this form shall be used by the CSO to report FCL actions to DISCO.

o. DD Form 555. "Central Index File Request" -- this form is prescribed for use by activities of UA's in requesting information concerning the PCL status of contractor personnel.

p. Reserved.

q. DISCO Form 562. "Personnel Security Clearance Change Notification" -- this multipurpose form is used by contractors to report clearance transfers, reemployment of cleared personnel, change of name, termination of employment, or administrative termination of clearances.

r. DD Form 696. "Industrial Security Inspection Report" -- the purpose of this report is to provide for uniform and comprehensive reporting of results of security inspections of facilities conducted to determine contractor compliance with the requirements of the ISM and such additional security requirements as may be provided for by individual contracts.

s. Reserved.

t. DISCO Form 703. This form is an envelope which is preaddressed to DISCO and used for submitting DD Forms 48, 48-3, and 49 to DISCO. It enables a clearance applicant to put the forms containing privileged information into the envelope and seal it.

u. DISCO Form 704. This form is a prepaid-postage envelope used for submitting DD Forms 48, 48-3, and 49 to the CSO in OODEP cases. Contractors are required to address the envelopes to their CSO's.

v. Reserved.

w. DIS Form 1148. "Industrial Security Survey/Inspection Report (Commercial Carrier)". (see paragraph 4-106 for additional information) -- the purpose of part I of this report is to: develop sufficient facts to permit an administrative determination to grant or deny a security clearance to a commercial carrier; develop information concerning changed conditions, such as a change of address or reorganization; and determine whether the HOF of the commercial carrier is subject to FOCI factors. The purpose of part II of the report is to provide for uniform and comprehensive security inspections of commercial carriers to determine compliance with the requirements of reference (b).

x. DIS Form 1149. "Department of Defense Transportation Security Agreement" -- this form is prescribed for use by the CSO in obtaining the formal agreement of management of the HOF of the commercial carrier to abide by reference (b).

y. DIS Form 1150. "Appendage to Department of Defense Transportation Security Agreement" -- this appendage will be used by management of the HOF of the carrier to indicate those terminals covered by the DIS Form 1149 and DD Form 441s. Once executed, the HOF of the carrier will use the DIS Form 1150 to accomplish additions, deletions, or changes in the terminals included in and covered by the DIS Form 1149.

z. DD Form 1540. "Registration for Scientific and Technical Information Services" -- this form is used to establish a requirement for the services of DTIC and should be submitted to that office.

aa. DD Form 1541. "Facility Clearance Register" -- this form replaces the DTIC Form 62 and is to be used for the purpose of certifying the FCL and safeguarding ability of a contractor to the DTIC.

bb. Letter Agreement to Safeguard Classified Information for an Employee Performing Consultant Services. This agreement shall be prepared and executed by contractors if they agree to accept responsibility for safeguarding classified information released to their employees who are furnishing consultant services.

cc. Letter of Notification of Facility Security Clearance for a Commercial Carrier. This letter is prescribed for use by a CSO to notify a carrier facility (HOF or terminal) that it has been granted a FCL.

Part 2. EXHIBITS OF FORMS

9-200 Purpose. The purpose of this section is to describe and exhibit those industrial security forms which are not exhibited in the ISM or its supplements on COMSEC and commercial carriers, (see references (a), (b), and (q)).

| <u>Form No.</u> | <u>Title</u> | <u>Para.</u> |
|-----------------|---|--------------|
| DD Form 374 | "Facility Security Clearance Survey" | 9-201 |
| DIS Form 553 | "Central Index File Card-Facility" | 9-202 |
| DD Form 555 | "Central Index File Request" | 9-203 |
| DD Form 696 | "Industrial Security Inspection Report" | 9-204 |
| DIS Form 1148 | "Industrial Security Survey/Inspection Report (Commercial Carrier)" | 9-206 |

9-201 "Facility Security Clearance Survey" (DD Form 374). The purpose of this survey is to determine that the facility is capable of properly safeguarding classified information for precontract negotiations, and that management at the facility is fully cognizant of the responsibilities involved in the safeguarding of classified information. This survey shall be completed by the CSO as a prerequisite to granting the FCL. A survey is also conducted when a cleared facility's physical location changes.

SAMPLE

| | | | |
|---|--|---|---|
| DEPARTMENT OF DEFENSE FACILITY SECURITY CLEARANCE SURVEY See Instructions on Reverse Side | | DATE _____ | FORM APPROVED OMB NO. 0704-0089 EXP. DATE: MAR 1984 |
| 1. NAME OF SPECIFIC FACILITY BEING SURVEYED | | STREET ADDRESS, CITY AND STATE | |
| 2. NAME OF COMPANY OPERATING THE FACILITY | | STREET ADDRESS, CITY AND STATE | |
| 3. NAME OF PARENT ORGANIZATION | | STREET ADDRESS, CITY AND STATE | |
| 4. NAME AND OFFICIAL TITLE OF PERSON RESPONSIBLE FOR SECURITY AT THE FACILITY | | 5. DATE COMPANY ORGANIZED | |
| 6. HAS THE FACILITY OR ITS PARENT ORGANIZATION EXECUTED A CERTIFICATE PERTAINING TO FOREIGN AFFILIATION (DD Form 441a)? <input type="checkbox"/> YES <input type="checkbox"/> NO | | 7. WHAT IS THE APPROXIMATE PERCENTAGE OF THE FACILITY'S EMPLOYEES WHO ARE FOREIGN NATIONALS OR IMMIGRANT ALIENS? _____% | |
| 8. INDICATE HIGHEST CLASSIFICATION OF INFORMATION FACILITY IS PHYSICALLY EQUIPPED TO SAFEGUARD FOR PRECONTRACT NEGOTIATIONS. <input type="checkbox"/> TOP SECRET <input type="checkbox"/> SECRET <input type="checkbox"/> CONFIDENTIAL <input type="checkbox"/> NONE | | | |
| 9. REMARKS (Explain any anomalies which require clarification. Include those corrective measures that must be accomplished and maintained to safeguard classified information of the same category as that of the facility security clearance being processed. Include any additional obser- vations which from a security standpoint may affect granting the facility security clearance.) (If more space is required attach additional sheets.) | | | |
| 10. SIGNATURE OF SECURITY OFFICE MAKING SURVEY | | ADDRESS | |
| 11. TYPED NAME AND TITLE OF OFFICIAL MAKING SURVEY | | SIGNATURE | |

SAMPLE

INSTRUCTIONS

This form is to be completed following a survey of the facility by a representative of the DIS assigned security cognizance of the facility. Its purpose is to: (1) determine the ability of the facility physically to safeguard classified information of the category involved in the clearance of the facility; (2) serve as a basis for advising management of the facility of those corrective measures that must be accomplished and maintained to safeguard classified information of the same category as that of the facility security clearance being processed; (3) Ascertain that DD Form 441a has been completed.

To the extent possible, information required on this form should be obtained as a result of observation by the representative of the cognizant security office. Some of this information will, of necessity, be obtained in conference with plant executives.

Where information cannot be fully recorded in the space provided on this form, a blank sheet of paper should be used and attached to the form and properly referenced by item number.

This form will be classified only when it contains classified information.

Explanation of Items:

1. Enter the name, number or other designation of the specific facility being surveyed and the facility's street address for purpose of indicating the exact physical location.

2. Enter the name and address of the company operating the facility, if such exists. If this is the same as Item 1, indicate "same".

3. Enter the name and address of the parent or home office organization, if such exists.

4. Enter the name and title of the official designated by company management to be responsible for safeguarding classified information.

5. Refer to the operating company (i.e., company identified in Item 2).

6. Indicate by check mark whether or not the company or parent or home office organization has executed a Certificate Pertaining to Foreign Affiliation (DD Form 441a).

7. Self-explanatory.

8. Evaluate the ability of the facility to safeguard classified information, and check the appropriate box to indicate the highest classification of information the facility is physically equipped to safeguard for present and future operations. This evaluation should be based upon the requirements for storage of classified security matter contained in the Department of Defense "Industrial Security Manual for Safeguarding Classified Information. (DD 441 attachment)".

DISTRIBUTION

1. Original to Central Index File.

2. Copy to the cognizant security office granting facility security clearance.

3. Copy to procuring activity requesting the facility security clearance (if appropriate).

4. Headquarters of the User Agency distribution is optional.

5. Copy to facility is not required.

9-202 "Central Index File Card-Facility" (DIS Form 553). This form shall be used by the CSO to report FCL actions to DISCO. The original of the form shall be retained in the CSO and one copy will be sent to the DTIC when appropriate. When the FCL action being reported is pending or interim in nature, the DIS Form 553 shall clearly indicate that fact. Illegible, incomplete, or incorrectly executed forms shall be returned to the originating activity for correction. Letters of transmittal are not required with the submission of DIS Form 553.

9-202.1 Checklist for the Preparation of DIS Form 553. In order to obtain maximum utilization of the information contained on DIS Form 553, and to provide for clarity of reproduction, only black ink or black type shall be used in preparing the original of these forms. DISCO may return these forms if a color other than black is used.

a. Item 1. Enter the name or other designation of the specific facility being cleared.

b. Item 1a. Enter the exact mailing address for the facility.

c. Item 2. Enter the level of clearance granted. If pending actions is being reported, strike out the word "granted" in the title of item 2, and insert the words "in process for" in the block, followed by the level of clearance being processed. If the facility has been granted or is in process for a FCL under a reciprocal agreement, the phrase "(country) RECI-PROCAL," as appropriate, shall be entered in this block in capital letters, following the level of clearance granted or being processed.

d. Item 2a. Enter the date clearance was granted. If in process, leave block blank.

e. Item 3. Enter the physical address of the facility (street number, city, state, or highway and location thereon, district, town, or county, and state), if different from the mailing address.

f. Item 4. Enter the name of the HOF, if the facility identified in block 1 is part of a MFO. If none exists, insert "None" and leave items 4a, 5, 5a, and 6 blank.

g. Item 4a. Enter the exact mailing address of the HOF.

h. Item 5. Enter the level of clearance granted the HOF. If pending action is being reported, strike out the word "granted" in the title of item 5, and insert the words "in process for" in the block, followed by the level of clearance being processed. If the facility has been granted or is in process for a reciprocal FCL, the appropriate phrase shall be entered in this block in capital letters, following the level of clearance granted or being processed. If the HOF is located in another region, inquiry must be made of the appropriate region to obtain the data required.

i. Item 5a. Enter the date clearance was granted. If in process, leave block blank.

j. Item 6. Enter the exact physical address of the HOF, if different from the mailing address.

k. Item 7. Enter the exact name of the parent organization, if such exists. If none exists, insert "None" and leave items 7a, 8, 8a, and 9 blank.

l. Item 7a. Enter the exact mailing address of the parent organization.

m. Item 8. Enter the level of clearance granted the parent organization. If pending action is being reported, strike out the word "granted" in the title of item 8, and insert the words "in process for" in the block, followed by the level of clearance being processed. If the parent organization has been granted or is in process for a reciprocal FCL, the appropriate phrase shall be entered in this block in capital letters, following the level of clearance granted or being processed. If the organization is excluded from access to all classified information to be released to the subsidiary, in accordance with the provisions of paragraph 2-104, insert the words, "Excluded from access," followed by the date the certificate of exclusion was submitted. If granted a clearance, but excluded from access to a higher category of information to be released to the subsidiary, enter the level of clearance granted, followed by the phrase, "Excluded from access to (enter appropriate category)," followed by the date certificate of exclusion was submitted. If the parent is located in another region, inquiry must be made of the appropriate region to obtain the data required.

n. Item 8a. Enter the date the FCL was granted. If in process, leave block blank.

o. Item 9. Enter the exact physical address of the parent organization, if different from mailing address.

p. Item 10. Check the appropriate box to indicate the type of action being reported. See examples below.

(1) When reporting a FCL action for the first time, check the box to indicate "initial card."

(2) If a DIS Form 553 is on file at DISCO, check the box to indicate the card supersedes DIS Form 553 previously submitted, and insert the date of previous card.

(3) When submitting a "pending" DIS Form 553, due to a change of name or physical location of a facility which has been previously granted a clearance, and processing to current status is still in progress, check the box to indicate initial card, and include in block 11 of the form a cross reference, by name and address, to the existing DIS Form 553 at DISCO and the specific reason for submission. When processing to current status is completed, a final DIS Form 553 shall be submitted to DISCO, superseding the previous "pending" DIS Form 553. Include in block 11 of the form an identical cross reference, by name and address, to the DIS Form 553 which was in DISCO before processing was initiated. This will ensure that DISCO will remove both of the existing DIS Forms 553 from its files.

(4) When submitting a DIS Form 553 due to a change of mailing address, where the physical location of a facility which has been previously cleared remains the same and it is possible to complete the processing to current status by following the provisions of paragraph 2-118c(2), a DIS Form 553, superseding the previous DIS Form 553 on file, shall be submitted. The reason for submission shall be set forth in block 11.

q. Item 11. A qualifying statement pertaining to action taken in accordance with the provisions of this regulation shall be entered in this block, if such conditions exists. In addition, this block shall be used to set forth necessary cross reference to existing DIS Form 553 at DISCO when required (see items 9-202.1p(3) and (4)).

r. Item 12. Self-explanatory

s. Item 12a. Self-explanatory

t. Item 12b. Insert date form is submitted.

u. Item 12c. Insert the appropriate numerical code number which identifies the CSO submitting the form.

(1) Termination of Facility Security Clearance. When conditions occur in a facility which permit administrative termination of the FCL, a DIS Form 553, with all available information recorded thereon, shall be submitted to DISCO, with a duplicate copy to DTIC, if appropriate. The reason for submission shall be set forth in item 11.

(2) Invalidation of Facility Security Clearance. When changed conditions occur in a facility which require invalidation of the FCL, a DIS Form 553, with all available information recorded thereon, shall be submitted to DISCO with a duplicate copy sent to DTIC, if appropriate. The reason for submission shall be set forth in item 11.

SAMPLE

| | | | |
|--|------------------|---|--------------------------|
| 1. FACILITY GRANTED CLEARANCE | | 1A. MAILING ADDRESS (Include ZIP Code) | |
| 2. CATEGORY OF CLEARANCE GRANTED | 3A. DATE CLEARED | 3. LOCATION (If different from 1a) | |
| 4. HOME OFFICE | | 4A. MAILING ADDRESS (Include ZIP Code) | |
| 5. CATEGORY OF CLEARANCE GRANTED | 5A. DATE CLEARED | 5. LOCATION (If different from 4a) | |
| 7. PARENT ORGANIZATION | | 7A. MAILING ADDRESS (Include ZIP Code) | |
| 8. CATEGORY OF CLEARANCE GRANTED | 8A. DATE CLEARED | 8. LOCATION (If different from 7a) | |
| 10. <input type="checkbox"/> INITIAL CARD <input type="checkbox"/> THIS CARD SUPERSEDES "CENTRAL INDEX FILE CARD - FACILITY" SUBMITTED ON (Date) _____ | | | |
| 11. REMARKS | | | |
| 12. TYPED NAME AND TITLE OF OFFICIAL SUBMITTING CARD | | 12A. SIGNATURE | 12B. DATE FORM SUBMITTED |
| | | | 12C. BY S _____ |
| DIS Form 553 Oct 63 | | Replaces DIS Form 553, Jan 61, which is obsolete. | |
| CENTRAL INDEX FILE CARD - FACILITY | | | |

9-203 "Central Index File Request" (DD Form 555). This form is prescribed for use by activities of UA's in requesting information concerning the PCL status of contractor personnel. Users of this form shall ensure that the individual about whom information is requested is identified correctly. Requests for information about individuals will be sent to DISCO, P.O. Box 2499, Columbus, Ohio 43216. Requests concerning facilities will be sent to the CSO in which the facility is located. The format of this form is designed for use with window envelopes. Return address must be placed in the lower left corner of the form. Letters of transmittal are not required.

9-203.1 Checklist for Preparation of DD Form 555.

a. The following items shall be completed by the requester.

- (1) Item 1. Self-explanatory
- (2) Item 2. Enter the full name of the person concerned.
- (3) Item 3. Self-explanatory
- (4) Item 4. Enter day, month, and year.
- (5) Item 5. Enter city and state, if born in U.S., or city and country, if foreign born.
- (6) Item 6. Enter country of current citizenship.
- (7) Item 7. Self-explanatory
- (8) Item 8. Enter street number, city, and state.
- (9) Item 9. Enter sufficient information to fully identify the exact facility where the individual concerned is employed.
- (10) Item 10. Enter the complete street and address, city, and state of the facility.
- (11) Item 11. If necessary, give any additional information or explanatory remarks pertinent to the individual.
- (12) Item 12. Indicate by a check mark in the box if need exists for a reproduced copy of the completed form.
- (13) Item 13. Type the name and position or rank of the official requesting the check.
- (14) Item 14. The requester will fill in the address of official or agency requiring the information, within the block "To:" -- this may be the same or different address than the requester. Zip code shall be included in the address.

b. The following items shall be completed by DISCO.

(1) Item 15. No record will be indicated in the appropriate box if such is the case.

(2) Item 16. Initials will be entered in the appropriate box by the individuals at DISCO who are furnishing the information.

SAMPLE

| CENTRAL INDEX FILE REQUEST | | | | DATE |
|---|-------------------|--|---|------|
| FROM: | | TO: DEFENSE INVESTIGATIVE SERVICE DEFENSE INDUSTRIAL SECURITY CLEARANCE OFFICE P. O. BOX 2489 COLUMBUS, OH 43216 | | |
| 1. REQUEST THAT A CHECK BE MADE OF THE RECORDS OF CENTRAL INDEX FILE OF THE PERSON NAMED BELOW: | | | | |
| PERSON | | | | |
| 2. NAME - LAST, FIRST, MIDDLE | | 3. ANY OTHER NAME(S) BY WHICH KNOWN (Nodan or Alias) | | |
| 4. DATE OF BIRTH | 5. PLACE OF BIRTH | 6. CITIZEN OF | 7. SOCIAL SECURITY NUMBER | |
| 8. RESIDENCE (Present address, including Zip Code) | | | | |
| 9. EMPLOYER | | 10. LOCATION OF PLANT WHERE EMPLOYED (Complete address) | | |
| 11. REMARKS | | | | |
| 12. REQUEST THAT A COPY OF DISCO FORM 555 BE FURNISHED | | | | |
| 13. TYPED NAME, GRADE/RANK AND TITLE OF OFFICER REQUESTING CHECK | | SIGNATURE | | |
| 14. RETURN ADDRESS, INCLUDING ZIP CODE (To be completed by Requestor) | | | 15. RESULTS OF CHECK | |
| <div style="text-align: center;"> <div>TO</div> <div>L</div> </div> | | | <input type="checkbox"/> NO RECORD <input type="checkbox"/> DISCO FORM 555 FURNISHED | |
| | | | 16. FOR THE CENTRAL INDEX FILE INITIALS | |

9-204 "Industrial Security Inspection Report" (DD Form 696). The purpose of the report is to provide for uniform and comprehensive facility inspection reports to determine whether contractors are complying with the requirements of the ISM and such additional security requirements as may be provided for by individual contracts. It is the vehicle by which the industrial security representative documents the scope and results of an inspection. One or more narrative pages will be attached to the DD Form 696 depending on the scope of a given inspection. The "Remarks" section of the DD Form 696 will include as a minimum:

a. a general description of any changes in business activity or organization/ownership of the facility which could impact on the ability of the facility to perform classified activities,

b. a completely detailed description of any deficiencies observed, and an equally detailed description of corrective action taken,

c. a detailed description of the action taken to correct any deficiencies which were unresolved at the completion of the previous inspection,

d. a description of any unusual or unique facets of the facility's security program, and

e. a complete discussion of any question or other area that merits a narrative. (NOTE: Generally a narrative is not required for questions answered in the affirmative.)

9-204.1 Guideline Questions for Industrial Security Inspections (DD Form 696). Appendix XIII, ISM, provides a listing of guideline questions designed to be used in conjunction with the DD Form 696. The questions are not considered to be a part of the DD Form 696. Each question should lead the industrial security representative to more detailed questions not contained in the listing in order to ensure complete coverage of all aspects of a given point.

9-204.2 Explanation of DD Form 696 Items. An explanation of pertinent administrative items on the DD Form 696 is as follows.

a. Item 1. "Name of Facility" -- insert the name of the facility inspected.

b. Item 5. "Facility Clearance Level" -- insert level of facility clearance as follows:

T - TOP SECRET
S - SECRET
C - CONFIDENTIAL

c. Item 5b. "Category of Facility" -- is a scoring system in accordance with procedures established in the DIS "Industrial Security Operating Manual" (ISOM) (reference (aaa)).

d. Item 7. "Type of Business" -- indicates whether manufacturing, research and development, graphic arts, consultant, or other type of business.

e. Item 15. "Scope of Inspection" -- regularly scheduled DIS inspections and initial inspections must always be complete, in-depth efforts. Accordingly, partial inspections are prohibited, except as provided for in reference (aaa).

f. Item 15b. "Results of Inspection" -- the following is an explanation of the abbreviations used.

- (1) No Def -- no deficiencies
- (2) COS -- deficiencies are corrected on the spot.
- (3) LOR -- letter of requirements which is sent to the contractor as a report on the results of the inspection.
- (4) Major -- identifies major deficiency(ies) at the facility.

g. Item 16a. Identify in item 20 specifics regarding any evidence of FOCI.

h. Item 16c. If counterintelligence awareness briefings have been given, as required by paragraph 5f, ISM, identify in item 20 the government activity that conducted the briefing, date held, and number of employees (including OODEPS) in attendance. Similar information is to be provided for a briefing by the FSO or designee.

i. Item 19. "Other DoD Programs" -- the following is an explanation of the abbreviation used:

- (1) AA&E -- arms, ammunition, and explosives
- (2) DIFPP -- Defense Industrial Facilities Protection Program

9-204.3 General Note for Personnel Processing This Report. Items marked with an asterisk (*) have been registered in the DoD Data Element Program. Data elements and coding must be as indicated in the instructions. In cases where specific coding instructions are not provided, reference must be made to the "Department of Defense Manual for Standard Data Elements," DoD 5000.12-M (reference (bbb)). Noncompliance with either the coding instructions contained herein or those registered in the DoD Data Element Program will make the organization which fails to comply responsible for the required concession in data base communication. Cost of data conversions will be borne by the manager whose category of data elements lack precedence. Items:

- a. *1. Address of Facility
- b. *1a. Federal Supply Code Number (FSC No.)
- c. *2. Address of Home Office
- d. *3. Address of Parent Holding Company
- e. *4. Name of Facility Security Supervisor
- f. *5. Facility Clearance Level
- g. *5a. Clearance Date
- h. *5b. Category of Facility
- i. *6. Dates of Inspection
- j. *9. Access to Classified Material Last Inspection
Date of Facility Clearance

- k. *15. Scope of Inspection
- l. *15a. Inspection Rating Assigned
- m. *15b. Results of Inspection
- n. *16. Elements of Inspection and Ratings Assigned
- o. *17. Safeguarding Ability
- p. *21. Name of Security Specialist(s)
- q. *22. Name of Reviewing Official Date of Review

SAMPLE

FOR OFFICIAL USE ONLY (When filled in)

| INDUSTRIAL SECURITY INSPECTION REPORT | | | | | DATE PREPARED (Year, Month, Day) | | FORM APPROVED OMB NO. 0704-0014 EXP. DATE: OCT 1986 | |
|--|--|---|--|--|---|--|---|---------------------------|
| 1. NAME OF FACILITY | | | 2. NAME OF HOME OFFICE (Multiple Facility Organization) | | | 3. NAME OF PARENT HOLDING COMPANY (Parent-Subsidiary Organization) | | |
| ADDRESS OF FACILITY (Street, City, State, Zip Code) | | | ADDRESS OF HOME OFFICE (Street, City, State, Zip Code) | | | ADDRESS OF PARENT HOLDING COMPANY (Street, City, State, Zip Code) | | |
| 1a. PFC NO. | | | 4a. TEL. NO. (Include area code) | | | 5a. FACILITY CLEARANCE LEVEL | | |
| 4. NAME OF FACILITY SECURITY SUPERVISOR (Last, First, MI) | | | 5b. CLEARANCE DATE (Yr, Mo., Day) | | | | | |
| 5b. CATEGORY OF FACILITY | 6. DATES OF INSPECTION (Yr., Mo., Day) | 7a. PREVIOUS | 7b. CURRENT | 7c. NEXT | 7. TYPE OF BUSINESS | | | |
| 8. TIME EXPENDED (In Hours) | | | | 9. ACCESS TO CLASSIFIED MATERIAL SINCE LAST INSPECTION | | | | |
| TRAVEL | RESEARCH AND PREPARATION | INSPECTION | POST INSPECTION (Report, letter, etc.) | YES | | NO | | LEVEL (T, S, or C) |
| | | | | POSSESSING | | | | DATE (Year Month, Day) |
| | | | | ACCESS ELSEWHERE | | | | |
| | | | | GRAPHIC ARTS | | | | |
| 10. TOTAL NUMBER OF EMPLOYEES | 11. NUMBER OF U. S. EMPLOYEES CLEARED | | | NO ACCESS (Dormant) | | | | |
| | 11a. TOP SECRET | 11b. SECRET | 11c. CONFIDENTIAL | NO ACCESS (Home Office) | | | | |
| | | | 11d. GOV'T COMPANY | NO ACCESS (Parent) | | | | |
| 12. NUMBER OF ALIENS | 13. NUMBER OF IMMIGRANT ALIENS CLEARED | | | 14. SPECIFY NUMBER AND COUNTRY REPRESENTED BY EMPLOYEES GRANTED RECIPROCAL CLEARANCES. | | | | |
| | 13a. SECRET | | | 13b. CONFIDENTIAL | | | | |
| 15. SCOPE OF INSPECTION | | 15a. INSPECTION RATING ASSIGNED | | 15b. RESULTS OF INSPECTION | | | | |
| <input type="checkbox"/> COMPLETE <input type="checkbox"/> PARTIAL | | <input type="checkbox"/> SATISFACTORY <input type="checkbox"/> UNSATISFACTORY | | <input type="checkbox"/> NO DEF <input type="checkbox"/> COS <input type="checkbox"/> LOR <input type="checkbox"/> MAJOR | | | | |
| 16. ELEMENTS OF INSPECTION AND RATINGS ASSIGNED (S - Satisfactory, U - Unsatisfactory, NA - Not Applicable) | | | | 17. SAFEGUARDING ABILITY (Top Secret, Secret, Confidential or None) | | | | |
| ALPHA CODE | AREAS INSPECTED | | RATINGS | PREVIOUS RATING | 17a. FOR DOCUMENTS | | 17b. FOR HARDWARE | |
| A | FACILITY CLEARANCE | | | | APPROVED STORAGE FACILITIES | | NUMBER | |
| B | ACCESS AUTHORIZATIONS | | | | | | | |
| C | SECURITY EDUCATION | | | | | | | |
| D | STANDARD PRACTICE PROCEDURES | | | | | | | |
| E | SUBCONTRACTING | | | | | | | |
| F | VISIT CONTROL | | | | | | | |
| G | CLASSIFICATION | | | | | | | |
| H | EMPLOYEE IDENTIFICATION | | | | | | | |
| I | FOREIGN TRAVEL | | | | | | | |
| J | PUBLIC RELEASES | | | | | | | |
| K | CLASSIFIED STORAGE | | | | | | | |
| L | MARRINGS | | | | | | | |
| M | TRANSMISSION | | | | | | | |
| N | CLASSIFIED MATERIAL CONTROLS | | | | | | | |
| O | CONTROLLED AREAS | | | | | | | |
| P | DISPOSITION | | | | | | | |
| Q | REPRODUCTION | | | | | | | |
| R | CLASSIFIED MEETINGS | | | | | | | |
| S | CONSULTANTS | | | | | | | |
| T | ADP | | | | | | | |
| U | COMSEC/CRYPTO | | | | | | | |
| V | INTERNATIONAL OPERATIONS | | | | | | | |
| | | | | | 19. OTHER DOD PROGRAMS | | | |
| | | | | | <input type="checkbox"/> AASE <input type="checkbox"/> DIPP <input type="checkbox"/> OTHER (List) | | | |

1/ A narrative type report which supports the entries in items 15, 16, and 17 shall be accomplished by using the "Remarks" block on reverse side, and if necessary, continue on a separate sheet of paper and attach to this report. The narrative report should be limited to include the Alpha Code for the area.

SAMPLE

20. **REMARKS** (Include deficiencies noted during inspection. Show specific deficiency, applicable ISM requirement and action taken, if any, to correct deficiencies before termination of inspection. Also indicate corrective action taken on previous deficiencies. In addition, a statement giving an evaluation of the contractor's security posture in relation to facilities of similar nature and size. Outstanding features should be noted, i.e. training program, document control etc. If none, so state. Include names and titles of key personnel interviewed during inspection. Indicate specific locations (covered by a single facility clearance) that were inspected. Continue on a separate sheet of paper when necessary.)

| | | |
|--|---|---|
| 21. NAME(S) OF SECURITY SPECIALIST(S) (TYPED OR PRINT) (Last, First, MI) | SIGNATURE(S) OF SECURITY SPECIALIST(S) | TEAM INSPECTION <input type="checkbox"/> YES <input type="checkbox"/> NO |
| 22. NAME OF REVIEWING OFFICIAL (TYPED OR PRINT) (Last, First, MI) | SIGNATURE OF REVIEWING OFFICIAL | DATE OF REVIEW (Yr Mo Day) |

9-206 "Industrial Security Survey/Inspection Report (Commercial Carrier)" (DIS Form 1148). The purpose of part I of this report is to develop sufficient facts and to ensure submission of necessary documents to permit an administrative determination to grant or deny a security clearance to a commercial carrier. In addition, part I is utilized to develop information concerning changed conditions such as a change of address or reorganization. Part I is also to be used by the CSO in determining whether the HOF of the commercial carrier is subject to FOCI factors. The information in part I and attachments thereto is used as an aid to investigation in such cases. The purpose of part II of the report, when used in conjunction with an approved inspection checklist, is to provide for uniform and comprehensive security inspections of commercial carriers to determine compliance with the requirements of reference (b). (See paragraph 4-106 for additional information.)

9-206.1 Instructions for Completing DIS Form 1148.

- a. Use "N/A" when an item is not applicable.
- b. Whenever part I is used, the original report with all attachments will be forwarded to DISCO. The CSO will retain a copy in its facility file folders. When part II is used, the CSO will retain a copy in the appropriate facility file folders, in order to have available the latest information pertaining to the security status of the facility. The information in part II is not intended for routine distribution; however, the CSO, on request, shall furnish advice as to the security status of the commercial carrier.
- c. Items 1 through 5, 7 through 9, 11 through 17, 22, 23, 25, and 26. Self-explanatory
- d. Item 6. If this date predates the current ISM, explain in narrative.
- e. Item 10. Include sufficient information to permit a CSO to reply readily to inquiries concerning safeguarding ability.
- f. Item 18. Only applicable during an initial survey
- g. Item 19. Obtain a copy of annual report to stockholders, if available, to assist in analysis of ownership and management.
- h. Item 20. Specify in attachment the areas covered in the indoctrination of management with special emphasis on general and reporting requirements and completion of required government forms.
- i. Item 21. Define the term "foreign interests" for the company officials and ensure that all aspects of company operation are explored to resolve the question of whether there is FOCI. Obtain a DD Form 441s from the commercial carrier.
- j. Item 24. Do not include minor defects, corrected on the spot, in letters of requirements; however, such defects should be included in the narrative report with an appropriate explanation.

SAMPLE

FOR OFFICIAL USE ONLY (when filled in)

| INDUSTRIAL SECURITY SURVEY/INSPECTION REPORT (COMMERCIAL CARRIER) | | | | DATE PREPARED | | FORM APPROVED ONS NO. 6784-0127 EXP. DATE: MAY 1984 | |
|---|--------------------------|--|--|---|--|---|--|
| 1. NAME, ADDRESS & ZIP CODE OF FACILITY | | 2. NAME, ADDRESS & ZIP CODE OF HOME OFFICE (Multiple Facility Organisation) | | 3. NAME, ADDRESS & ZIP CODE OF PARENT HOLDING COMPANY (Parent-Subsidiary Organisation) | | | |
| 4. NAME OF FACILITY SECURITY SUPERVISOR | | 4a. TELEPHONE NO. | | 5. TYPE OF BUSINESS | | | |
| 6. DATE OF STANDARD PRACTICE PROCEDURES | | 7. CLEARANCE a. LEVEL b. DATE | | 8. SECURITY EVALUATION IS <input type="checkbox"/> SATISFACTORY <input type="checkbox"/> UNSATISFACTORY | | | |
| 9. TIME EXPENDED (In Hours) | | | | 10. SAFEGUARDING ABILITY (State Briefly) | | | |
| TRAVEL | RESEARCH AND PREPARATION | SURVEY/ INSPECTION | POST INSPECTION (Report, letter, etc.) | DOCUMENTS | | | |
| | | | | HARDWARE | | | |
| 11. TOTAL NUMBER OF EMPLOYEES | | 12. NUMBER OF U. S. EMPLOYEES CLEARED a. TOP SECRET b. SECRET c. CONFIDENTIAL d. GOV'T e. COMPANY | | 13. NUMBER OF ALIENS | | 14. NUMBER OF ALIENS CLEARED a. TOP SECRET b. SECRET c. CONFIDENTIAL | |
| 15. NUMBER OF EMPLOYEES GRANTED | | | | 16. USE DECLASSIFICATIONS | | | |
| a. UNITED KINGDOM RECIPROCAL CLEARANCES | | | | b. CANADIAN RECIPROCAL CLEARANCES | | | |
| PART I - SURVEY <u>/</u> | | | | | | | |
| (This part shall be completed when conducting an initial survey or one required by changed conditions) | | | | | | | |
| 16. TYPE OF SURVEY: <input type="checkbox"/> INITIAL <input type="checkbox"/> CHANGED CONDITION | | | | | | | |
| 17. REASON FOR SURVEY TO INCLUDE IDENTITY OF REQUESTER OR BASIS FOR ACTION. | | | | | | | |
| 18. HISTORY (Name and address changes for preceding ten years, type of business, organization structure, number of non-citizen employees). | | | | | | | |
| 19. ANALYSIS OF OWNERSHIP AND MANAGEMENT (Attach list of OODEPs, indicate voting stock distribution and percent held by non-citizens and total number of directors constituting legal quorum). | | | | | | | |
| 20. INDOCTRINATION OF MANAGEMENT. | | | | | | | |
| 21. IS THERE FOREIGN OWNERSHIP CONTROL OR INFLUENCE (FOCI)? <input type="checkbox"/> YES <input type="checkbox"/> NO. (If YES, check the appropriate box below and describe contractor's plan to nullify foreign influence factors or a notation that facility does not desire to submit a plan. Specify legal documentation required). <input type="checkbox"/> STOCK OWNERSHIP (Over 5%) <input type="checkbox"/> INTERLOCKING DIRECTORATES <input type="checkbox"/> AGREEMENTS OR JOINT VENTURES <input type="checkbox"/> CONTROL OR INFLUENCE OVER MANAGEMENT <input type="checkbox"/> FOREIGN OODEPs <input type="checkbox"/> INDEBTEDNESS <input type="checkbox"/> OTHER (Specify) | | | | | | | |
| PART II - INSPECTION <u>/</u> | | | | | | | |
| (This part will be completed for recurring inspections) | | | | | | | |
| 22. PRE-INSPECTION PLANNING (Indicate extent), I. E., DO FORM 254, ADMINISTRATIVE INQUIRIES, SPP, PLAN OF INSPECTION. | | | | | | | |
| 23. INSPECTION (Indicate scope, organizational elements, areas or buildings covered. Select questions from inspection check list in DISM 51-4 which are applicable to facility. Cite deficiencies, paragraph of Industrial Security Manual and Standard Practice Procedures not complied with, corrective action necessary. Also indicate corrective action taken on previous deficiencies). | | | | | | | |
| 24. POST INSPECTION (Identify management officials criticized, deficiencies which should be included in letter of requirements, and degree of follow-up action required). | | | | | | | |
| PART III - CERTIFICATION | | | | | | | |
| I CERTIFY that the entries made by me in Part I or II above and attached sheets are correct to the best of my knowledge and belief. | | | | | | | |
| 25. TYPE, OR PRINTED NAME OF INDUSTRIAL SECURITY REPRESENTATIVE | | | | 25a. SIGNATURE OF INDUSTRIAL SECURITY REPRESENTATIVE | | | |
| 26. DATES OF SURVEY INSPECTION | | | | | | | |
| a. PREVIOUS | | b. CURRENT | | c. NEXT | | | |
| <u>/</u> A narrative type report which covers the elements of information requested, shall be attached to and made a part of this report | | | | | | | |

SECTION X. OPERATIONS SECURITY (OPSEC)

10-100 Purpose. This section provides information and instructions for uniform implementation of the DoD OPSEC program within the Defense Industrial Security Program. *

10-101 General. The OPSEC program is a DoD directed effort, the mechanics of which are outlined in DoD Directive 5205.2 (DoD Operations Security Program, July 7, 1983). *

a. The principal objective of OPSEC is to preclude the disclosure of classified information by denying or reducing the opportunity of hostile intelligence services (HOIS) to gain access by directly observing/analyzing/evaluating our activities and operations, the awareness of which may lead to the compromise of classified information. Stated another way, OPSEC is the process of denying information about friendly intentions, capabilities, plans, or programs by identifying, controlling, and protecting intelligence indicators associated with planning and conducting military operations as well as other defense activities. *

b. Within the context of industrial security, the general aim of OPSEC is to promote mission effectiveness by preserving essential secrecy about U.S. intentions, capabilities, and current activities when the DISP procedures for safeguarding classified material and information require enhancement. Secrecy essential to defense activities may be compromised whenever open sources (such as technical articles, press releases, National Technical Information Service publications, the Congressional Record, Commerce Business Daily, or contract awards) and detectable activities (such as communications, logistics actions, research, development and test activities, or radar emissions) provide information that can be pieced together or analyzed, to the detriment of U.S. interests. In some instances, such information or indicators are not addressed by DISP requirements for classified material and require in-depth analysis and case-by-case planning to identify them. The fundamental goal of the OPSEC process is to minimize or eliminate such indicators. OPSEC thus encompasses activities which are unique to the OPSEC process, i.e., (a) determining, through threat/vulnerability analysis, whether there are unacceptable/undesirable intelligence indicators and what they are; and (b) developing and implementing countermeasures to best eliminate or minimize them. *

c. Contracts limited to classified information (such as those to process or evaluate information and produce classified documents, pictures, computer programs, training aids, and similar matters; for classified consultant, library, or ADP services; or for printing classified documents) generally do not require OPSEC. Contracts that involve system acquisition (such as those for weapon systems, Electronic Countermeasures, radio transmitters, active sensors, or low observable capabilities) or sensitive activities (such as intelligence operations or testing foreign material) usually require OPSEC, particularly if such contracts involve special access. Contracts for such things as logistics support, personal or maintenance services, may or may not require OPSEC, depending on the situation. *

d. OPSEC uses the same security measures that have been used to protect government information for years under the DISP but adds a new dimension. This new dimension or emphasis is the analysis, control and security of unclassified intelligence indicators. The object of this analysis and control is the protection of things we do, our operations, tests, and activities. As such, OPSEC is intended to complement the DISP.

e. The application of OPSEC measures supports the delicate balance between the need for secrecy, and the need to accomplish potentially detectable essential actions. This balance is threatened by the pervasive nature of the multidisciplined foreign intelligence activities directed against the U.S. The OPSEC process requires recognition of the intelligence threat, incorporation of OPSEC considerations into all stages of planning, and the application of appropriate protective measures. Effective OPSEC provides the best assurance that essential secrecy and surprise can be retained while denying the adversary an opportunity to develop effective countermeasures.

10-102 Application. The DoD OPSEC program is applicable only to Defense contractors participating in the DISP when the contracting User Agency determines that additional OPSEC measures are essential to protect classified information for specific classified contracts and imposes OPSEC as a contractual requirement. OPSEC is concerned with all sources of exploitable information. The DISP generally covers only the classified information disclosure problem, while OPSEC covers the total problem by addressing vulnerabilities and countermeasures for a specific program. OPSEC is principally oriented to those instances in which evaluations indicate program weaknesses which could lead to the disclosure of classified information.

a. OPSEC will be directed to the protection of unclassified intelligence indicators on classified programs of such nature that the disclosure of the indicators may lead to the compromise of classified information. OPSEC is not intended as a vehicle to protect unclassified technology; other programs exist to protect this information (DoD 5230.25).

b. Requirements for OPSEC shall be included in the appropriate requisition documentation and resultant contract or addendum thereto in sufficient detail to ensure complete contractor understanding of exactly what special OPSEC provisions are required by the UA. Full disclosure of these requirements is essential so that contractors can comply and charge attendant costs to the specific contracts for which they have been ordered. In providing such requirements, UA's shall not solely refer to their internal regulations when imposing OPSEC requirements, but shall fully specify the particulars in the contract proper, and shall provide full information necessary to explain internal regulations. Additionally, applicable DD 254s shall be annotated to indicate that OPSEC requirements are contained in the contract or addendum thereto.

c. Contractual OPSEC requirements shall be strictly limited to those sensitive projects which clearly justify extraordinary security measures beyond those embodied in the DISP as outlined in the ISM. If the ISM provides a countermeasure or safeguard for a particular identified vulnerability concern, the ISM will be allowed to address it and

redundant countermeasures will not be added as contractual OPSEC requirements (e.g. information, physical or personnel security). UAs shall make this determination prior to imposing OPSEC measures. Assistance in this area is available to UAs from CSO's. Further, OPSEC requirements shall be based on the most current UA hostile intelligence threat and vulnerability assessment available, keyed to specific contractor areas, processes, activities, or facilities involved in classified contract performance.

d. DIS shall have principal responsibility for inspecting contractor compliance with OPSEC requirements. DIS may, however, be accompanied by cognizant UA representatives if requested. Visits by representatives of DoD Components to DISP facilities for OPSEC purposes will be coordinated with the Cognizant (Cog) DIS Office of Industrial Security (as much lead time as possible should be allowed). A representative of the Cog office may accompany the component member on the visit to the contractor; however, depending on the nature of visit, it will not always be necessary for the Cog office representative to be present. UA changes in OPSEC plans or requirements as a result of UA visits or evaluations will be provided to the Cog office.

e. DIS OPSEC inspections of contractors performing on classified contracts aboard military installations shall be performed only when requested by installation commanders.

10-103 Responsibilities.

a. UA procuring activities shall:

(1) If determined necessary to impose OPSEC measures, ensure that specific, detailed requirements for OPSEC are incorporated into any solicitation, and any resulting contract, subcontract, or addendum thereto so that the contractor will have a complete understanding of exactly what special security requirements in excess of ISM procedures are required by the User Agency. Full disclosure of these requirements is essential so that the contractor can comply with the contract provisions. DD Forms 254 shall not be used for this purpose; however, they shall indicate that OPSEC requirements are provided for in the applicable contracts.

(2) Provide the CSO full and detailed particulars of OPSEC requirements/measures and the DD 254s in each instance when such requirements are included in a classified contract awarded to industry. These include copies of the contract statement of work (SOW) when OPSEC requirements are included in such statement, UA approved OPSEC plans and requirements if contractually required, DD Form 1644, "Data Item Description, and DD Form 1423, "Contract Data Requirements List" (when these forms are used to convey OPSEC information or direct contractor submission of OPSEC documents/plans), etc. This information is needed to enable the CSO to inspect for compliance with OPSEC requirements during regularly scheduled DISP inspections.

(3) To the extent feasible, accompany and provide assistance *
when requested, to the CSO during regularly scheduled security inspections *
for assessment of compliance with contractually incorporated OPSEC measures. *

b. CSO shall: *

(1) Designate an OPSEC Coordinator who will be the point of *
contact for OPSEC matters within the Region. *

(2) Inspect contractor facilities when OPSEC requirements *
have been contractually incorporated into classified contracts to assess *
contractor compliance with the OPSEC requirements. These shall be *
accomplished: a) as part of a regularly scheduled industrial security *
inspection, b) as part of an unannounced industrial security inspection. *

(3) Request the UA Contracting Officer to provide assis- *
tance in the conduct of OPSEC inspections when deemed appropriate. *

(4) Coordinate visits by representatives of UA Contracting *
Officers to DISP facilities for OPSEC purposes. Every effort will be made *
to cooperate with the component in accommodating the visit. *

10-104. Procedures for Inspecting OPSEC Programs. *

a. CSOs will use the approved OPSEC Plan/Requirements provided *
them by the UA Contracting Officer as the basis for OPSEC inspections. *

b. When appropriate, the CSO will request a representative of *
the UA Contracting Officer to accompany IS Reps during inspections of *
industry OPSEC programs. *

c. Deficiencies of OPSEC contract requirements identified *
during joint DIS/contracting office visits will be discussed between the *
IS Rep and the contracting office representative before the briefing to *
management and prior to citing the contractor for noncompliance. *

d. Deficiencies requiring remedial action identified during *
the inspection of a contractor's OPSEC program will be included in the LOR *
issued to the facility. Specific contract OPSEC requirements will be cited *
as the basis for identified deficiencies. *

e. Satisfactory OPSEC inspection results shall not be routinely *
distributed to UAs or the contracting offices having procurement responsi- *
bilities at the inspected facilities. However, when remedial action is *
required, the CSO shall furnish a copy of the inspection report to the UA *
concerned. *

APPENDIX A. RELEASE OF ECONOMIC AND TECHNICAL INFORMATION

A-100 Application. This appendix furnishes information on various subjects which the inspector will include in his or her initial and continuing advice and guidance to management.

A-101 Release of Economic and Technical Information. The ISM establishes uniform security practices within industrial plants for the protection of classified information. On the other hand, considerable information of value to a potential enemy is generated in the daily business of the nation, and particularly within industry, which receives no security classification until or unless the government acquires a proprietary interest in the subject matter. This information is passed freely in various forms. Management, on being informed, may institute a voluntary program governing the release of such unclassified information, if so desired.

a. Management of facilities should be encouraged by the inspector to exercise considerable caution prior to any release of unclassified economic or technical information in press releases, advertisements, notices to stockholders, annual or quarterly reports, brochures, and so forth, including reports in response to questionnaires from unknown or questionable sources. Management should be advised that indiscriminate release could make the job of the saboteur easier, by pointing out potential targets. Furthermore, this material when assembled, collocated, and evaluated, could also contribute materially to an accurate appraisal of the strategic intentions of the U.S. Among the various areas where management should exercise caution before making information public are the following:

- (1) contract award information;
- (2) vulnerable points within a manufacturing plant;
- (3) plans and details of expansion of equipment and facilities;
- (4) production methods, techniques, and equipment;
- (5) figures on production and production capacity of plants and units within plants;
- (6) sources of semifinished products, components, and supplies;
- (7) sources of power, other utilities, and critical transportation affecting plant operations;
- (8) information concerning the security protection of the plant; and
- (9) information concerning research and development activities.

b. An approved method to guard against assembling of this vital information by a potential enemy is to make management aware of the danger, and to determine at the source those details which may or may not involve questions of security. In such a manner, publication of those segments of information, which either in and of themselves, or the cumulative totals of which would be of significant intelligence value to a potential enemy, can be prevented. Any questions concerning the release of such information should be referred to the CSO.

c. Management should be further informed that if it has contracts with the DoD, the release of certain classes of information is covered by the provisions of current public information security guidances and paragraph 50, ISM. If the data or information pertains to technology or science and is unclassified and further concerns arms, ammunition, and implements of war, the Department of State, ITAR (reference (1)) applies. If the information was directly contracted for or derived from UA sources, project developments, studies, aid requirements, or contracted arrangements, the UA's requirements will apply. If the technical information concerns economic factors with strategic overtones, the Export Administration Act of 1979, administered by the Department of Commerce, applies.

d. Management should be advised that under no circumstances will it release to unauthorized persons classified information furnished to, or developed by, the facility and furthermore, that this restriction applies to releases to public media and representatives thereof.

A-102 Replying to Questionnaires.

a. The numbers and types of questionnaires being circulated throughout industry have increased considerably in recent years. There is no question as to the responsibilities of individuals making out such questionnaires when answers given would compromise classified defense information -- classified information cannot be released.

b. Assuming the provisions of paragraph 50, ISM, are inapplicable it is difficult to determine where to draw the line with respect to unclassified information which, in the aggregate, may have intelligence or strategic significance when published in synopsis form. Whether certain compilations of information would be considered classified or whether their release in unclassified form would have an adverse effect on the national security are questions that can be answered only after each case has been reviewed on its own merits. Is the activity circulating the questionnaire known to the recipient? Or is it a "front" for an activity whose motives are subject to question? What use is to be made of the material collected by the questionnaire? It might seem that the information requested on the questionnaire is available from unclassified publications. Often the only basic difference between these unclassified publications and the questionnaires is that such publications give factual data whereas the questionnaires seek subjective qualitative analyses of these facts. In any event, while data responses to questionnaires would be unclassified, unless someone commits a security violation, the use of such questionnaires is considered to be an excellent device to attempt to elicit the disclosure of classified information.

c. With the exception of paragraph 5o, ISM, there is no specific DoD regulation or prohibition against the filling out of such questionnaires, nor is it the policy of the DoD to direct companies or individuals to refrain completely from answering any and all questionnaires. Industry action in this regard must be voluntary. It is believed, however, that in leaving such matters to the individual discretion of the companies and individuals concerned, the exercise of common sense and good judgement will dictate the maintenance of a conservative outlook toward such matters. The DoD has no desire to interfere in legitimate business enterprise nor to impede the flow of information which might be expected to enhance the overall defense effort. The government realizes that industry itself has a heavy stake in protecting its proprietary interests and in winning deserved positions in the competitive market. How this can best be done is a matter for prudence and sound judgment. When in doubt, or in need of advice, in the exercise of their discretion in this matter, contractors may seek guidance from their CSO's. In any event, it would be appropriate for contractors to furnish copies of questionnaires seeking information of the nature discussed in paragraph A-103 below, to their CSO's for referral to the appropriate investigative agencies.

d. Questionnaires submitted by, or under the sponsorship of, agencies of the executive branch of the federal government should be complied with when there is evidence that the request has been approved by the Bureau of the Budget under the Federal Reports Act of 1942 (reference (ccc)). While there are certain exceptions to this act, such as tax forms and inquiries from Congressional committees, this is a safe guide to follow. This also applies to the collection of information by commercial research and management organizations, trade and business associations and organizations, university research groups, and the like, when representing themselves as agents of the government. Bureau of the Budget approval is evidenced in a letter by appropriate language citing a numerical symbol, and on a form by the following words and a numerical symbol usually placed in the upper right-hand corner:

FORM APPROVED

OMB NO. _____

EXP. DATE: _____

A-103 Requests from Communist Countries for Unclassified Information of Strategic, Scientific, and Technical Intelligence Value.

a. In addition to the passive collection effort described above, the Communist intelligence apparatus is engaged in an overt attempt to obtain unclassified information of strategic and technical intelligence value from U.S. industry, including DoD contractors. To accomplish this collection effort, the Communist intelligence personnel, working through numerous sources, send correspondence to industry requesting information in various forms, such as brochures, catalogs, books, productions charts, blueprints, layouts, technical and research reports, aerial photography, and maps. Firms may receive such requests originating from several identifiable sources: Communist countries and regions, and their embassies, missions, consulate, and the like; or from Communist agents registered with the DoD under the Foreign Agents Registration Act of 1938 (reference (ddd)) as representatives of principals within Communist countries. The footnote to paragraph 5u, ISM, lists the Communist countries.

b. Requests may also be received from sources not readily identifiable with Communist agents located within a neutral or friendly country or from sources who, while requesting information overtly, do not identify the principals for whom they are working. On occasion, the type of information requested or the nature of the request may indicate that the requester is acting on behalf of a Communist country. Also on occasion, the requester will offer Communist information in exchange for the U.S. information requested.

c. Whenever the provisions of paragraph 5o, ISM, do not apply, contractors may adhere to the following guidance.

(1) Communist personnel (such as military attaches) officially accredited to the U.S. are required to identify themselves when they make requests for information. If the contractor has reason to believe that such individuals made requests for information and failed to identify themselves, or incompletely identified themselves, the incident should be reported to the CSO and the nearest FBI field office.

(2) All requests for unclassified information originating from sources identified or suspected as being from Communist countries should be forwarded to the CSO for referral to the investigative agencies, as appropriate. Use one of the following addresses for the military department whose contract is involved: *

HQ Dept. of the Army *
The Pentagon *
ATTN: DAMI-CIS *
Washington, D.C. 20310 *

Office of Naval Intelligence *
Dept. of the Navy *
The Pentagon *
Washington, D.C. 20350 *

Assistant Chief of Staff, Intelligence *
Dept. of the Air Force *
The Pentagon *
Washington, D.C. 20330 *

A-104 Industrial Security and Communist Espionage. *

a. The Communist intelligence services are constantly on the alert for opportunities to gain any kind of advantage that can be exploited. Not all information desired is classified, and they can collect unclassified information through overt methods. One of the results of the freedom of a democratic society such as the U.S. is the availability of voluminous information to the public merely for the asking. The FBI reports there are approximately 2000 official Communist personnel stationed in Communist bloc embassies, consulates, trade delegations and missions throughout the United States. These people are accompanied by approximately 2000 dependents, many of whom have an espionage potential. This does not include those Communist representatives and their dependents who are temporarily in the country, *

such as members of delegations, commercial visitors, research scientists and the like. As of December 31, 1979, it is estimated that about 15,000 from Communist bloc countries visit the U.S. each year including many who are experts in the overt collection of public information. These figures do not include 240 officials from the People's Republic of China in the U.S. who are accompanied by 9 dependents. Further, as of this same date, an average of 500 representatives for the People's Republic of China were in this country in a temporary basis. It should be noted here that being able to secure material legally and so easily has the added advantage of eliminating the hazardous and time-and-personnel consuming clandestine operations which would otherwise be necessary. *

b. For the purpose of identifying that material categorized as intelligence information, the following definitions given in the "Department of Defense Dictionary of Military and Associated Terms" (JCS Pub 1) (reference (eee)) might best be quoted:

(1) Information (intelligence) is "unprocessed material of every description including that derived from observations, reports, rumors, photographs, etc., which when analyzed, produces intelligence."

(2) Intelligence is "the product resulting from the collection, evaluation, analysis, integration, and interpretation of all available information which concerns one or more aspects of foreign nations or of areas of operations and which is immediately or potentially significant to military planning and operations."

(3) Strategic intelligence is "intelligence which is required for the formation of policy and military plans at national and international levels."

(4) Scientific and technical intelligence is "the product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information which covers: a. foreign developments in basic and applied research, and in applied engineering techniques; and b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems and material, the research and development related thereto, and the production methods employed for their manufacture."

c. The seriousness of the situation has been recognized by the DoD and in order to preclude the dissemination of unclassified information regarding classified contracts by industrial firms, the procedures outlined in paragraph 5o, ISM, have been prescribed.

DISCO, DISI, AND OISI



OPERATIONAL AREAS OF DIS COGNIZANT SECURITY OFFICES

Capital Region (S1510)

The Capital Region includes the state of Virginia, Washington, D.C., and the counties of Harford, Baltimore, Howard, Anne Arundel, Montgomery, Prince Georges, Calvert, Saint Marys, and Charles in Maryland.

Mid-Atlantic Region (S1410)

The Mid-Atlantic Region includes the states of: Pennsylvania, Delaware, West Virginia, New Jersey, and Maryland (less the counties of Harford, Baltimore, Howard, Anne Arundel, Montgomery, Prince Georges, Calvert, Saint Marys, and Charles); and the following counties in New York:

| | |
|----------------------|-------------|
| Bronx | Queens |
| Kings (Brooklyn) | Richmond |
| Nassau | Rockland |
| New York (Manhattan) | Suffolk |
| Orange | Westchester |
| Putnam | |

Mid-Western Region (S3210)

The Mid-Western Region includes the states of: Ohio, Kentucky, Indiana, Michigan, Iowa, Minnesota, Nebraska, North Dakota, South Dakota, and Wisconsin; and the following counties in Illinois:

| | |
|------------|------------|
| Adams | Henderson |
| Boone | Henry |
| Brown | Iroquois |
| Bureau | Jasper |
| Carroll | Jo Daviess |
| Cass | Kane |
| Champaign | Kankakee |
| Christian | Kendall |
| Clark | Knox |
| Coles | Lake |
| Cook | La Salle |
| Crawford | Lee |
| Cumberland | Livingston |
| De Kalb | Logan |
| De Witt | Macon |
| Douglas | Marshall |
| Du Page | Mason |
| Edgar | McDonough |
| Effingham | McHenry |
| Ford | McLean |
| Fulton | Menard |
| Grundy | Mercer |
| Hancock | Morgan |

Mid-Western Region (S3210) (Continued)

| | |
|-------------|------------|
| Moultrie | Shelby |
| Ogle | Stark |
| Peoria | Stephenson |
| Platt | Tazewell |
| Pike | Vermillion |
| Putnam | Warren |
| Rock Island | Whiteside |
| Sangamon | Will |
| Schuyler | Winnebago |
| Scott | Woodford |

New England Region (S1110)

The New England Region includes the states of: Maine, New Hampshire, Vermont, Massachusetts, Rhode Island, and Connecticut; and the following counties in New York:

| | |
|-------------|----------------|
| Albany | Montgomery |
| Allegany | Niagara |
| Broome | Oneida |
| Cattaraugus | Onandaga |
| Cayuga | Ontario |
| Chautauqua | Orleans |
| Chemung | Oswego |
| Chenango | Otsego |
| Clinton | Rensselaer |
| Columbia | Saint Lawrence |
| Cortland | Saratoga |
| Delaware | Schenectady |
| Dutchess | Schoharie |
| Erie | Schuyler |
| Essex | Seneca |
| Franklin | Steuben |
| Fulton | Sullivan |
| Genesee | Tioga |
| Greene | Tompkins |
| Hamilton | Ulster |
| Jefferson | Warren |
| Kerkiraer | Washington |
| Lewis | Wayne |
| Livingston | Wyoming |
| Madison | Yates |
| Monroe | |

Northwestern Region (S5210)

The Northwestern Region includes the states of: Alaska, Idaho, Montana, Nevada, Oregon, Utah, Washington, and Wyoming; and the following counties in California:

| | |
|--------------|---------------|
| Alameda | Nevada |
| Alpine | Placer |
| Amador | Plumas |
| Butte | Sacramento |
| Calaveras | San Benito |
| Colusa | San Francisco |
| Contra Costa | San Joaquin |
| Del Norte | San Mateo |
| El Dorado | Santa Clara |
| Fresno | Santa Cruz |
| Glen | Shasta |
| Humboldt | Sierra |
| Inyo | Siskiyou |
| Kings | Solano |
| Lake | Sonoma |
| Lassen | Stanislaus |
| Madera | Sutter |
| Marin | Tehama |
| Mariposa | Trinity |
| Mendocino | Tulare |
| Merced | Tuolumne |
| Modoc | Yolo |
| Mono | Yuba |
| Monterey | |
| Napa | |

Pacific Region (S5310)

The Pacific Region includes the state of Hawaii, U.S. possessions & trust territories in the Pacific area, and the following counties in California:

| | |
|-------------|-----------------|
| Imperial | San Bernardino |
| Kern | San Diego |
| Los Angeles | San Luis Obispo |
| Orange | Santa Barbara |
| Riverside | Ventura |

Southeastern Region (S1410)

The Southeastern Region includes the states of: Alabama, Arkansas, Florida, Georgia, Louisiana, Mississippi, North Carolina, South Carolina, and Tennessee. It also includes Puerto Rico and U.S. possessions in the Atlantic and Caribbean areas.

Southwestern Region (S4210)

The Southwestern Region includes the states of: Arizona, New Mexico, Oklahoma, Texas, Colorado, Kansas, Missouri; and the following counties in Illinois:

| | |
|-----------|------------|
| Alexander | Madison |
| Bond | Marion |
| Calhoun | Massac |
| Clay | Monroe |
| Clinton | Montgomery |
| Edwards | Perry |
| Fayette | Pope |
| Franklin | Pulaski |
| Gallatin | Randolph |
| Greene | Richland |
| Hamilton | St. Clair |
| Hardin | Saline |
| Jackson | Union |
| Jefferson | Wabash |
| Jersey | Washington |
| Johnson | Wayne |
| Lawrence | White |
| Macoupin | Williamson |

TELEPHONE NUMBERS AND ADDRESSES

The following listing contains the addresses and telephone numbers of the PIC-CVA and the CSO's. The following indicated numbers and addresses shall be used to obtain the required verification of facility clearance and safe-guarding capability of prospective contractors and subcontractors (see paragraphs 1-110, 1-111, 1-111.1, 1-409, and 2-118j). Correspondence should be addressed to the Defense Investigative Service, Director of Industrial Security (appropriate address as cited below).

| | <u>Address</u> | <u>Area Code</u> | <u>Telephone Number</u> | <u>AUTOVON NO.</u> |
|---------------------|---|------------------|---|--------------------|
| PIC-CVA | P.O. Box 1211 Baltimore, MD 21203-1211 | 301 | 633-4820 | |
| Capital Region | 2461 Eisenhower Avenue Alexandria, VA 22331 | 202 | 325-9616 | 221-9616 |
| Mid-Atlantic Region | 1040 Kings Highway North Cherry Hill, NJ 08034-1908 | 609 | 482-6500 (ask for clearance verification) | |
| Mid-Western Region | Federal Office Bldg. 1240 East 9th Street Cleveland, OH 44199 | 216 | 522-5338/9 | 580-5338/9 |
| New England Region | Barnes Building 495 Summer Street Boston, MA 02210 | 617 | 451-4927/3052 | 955-4927/3052 |
| Northwestern Region | Presidio of San Francisco San Francisco, CA 94129 | 415 | 561-3251 | 586-3251 |
| Pacific Region | 3605 Long Beach Blvd., Suite 405 Long Beach, CA 90807 | 213 | 595-7644/52 | |
| Southeastern Region | 805 Walker Street Marietta, GA 30060 | 404 | 429-6340 | 697-6340 |
| Southwestern Region | 1136 Washington Avenue St. Louis, MO 63101 | 314 | 263-6581/2/3 | 693-6581/2/3 |

DoD 5220.22-R

The following are the telephone numbers for the DIS Directors of Industrial Security. These numbers may be used for all matters other than verifications of facility clearances and safeguarding ability. The mailing address is the same as that listed above.

CSO Region

| | <u>Area Code</u> | <u>Telephone Number</u> | <u>AUTOVON NO.</u> (For Gov't. Agencies Use) |
|--------------|------------------|-------------------------|---|
| Capital | 202 | 325-9634/5 | 221-9634/5 |
| Mid-Atlantic | 609 | 482-6500 | |
| Mid-Western | 216 | 522-5334/5 | 580-5334/5 |
| New England | 617 | 451-4914/6 | 955-4914/6 |
| Northwestern | 415 | 561-3235/6 | 586-3235/6 |
| Pacific | 213 | 595-7251 | |
| Southeastern | 404 | 429-6330 | 697-6330 |
| Southwestern | 314 | 263-6580 | 693-6580 |

The following listing contains the addresses and telephone numbers of DISCO, DSI, and OISI. *

City & State

| | <u>Address</u> | <u>Area Code</u> | <u>Telephone Number</u> | <u>AUTOVON NO.</u> (For Gov't. Agencies Use) |
|-------------------|---|------------------|---|---|
| Columbus, OH | Director, DISCO, P.O. Box 2499 Columbus, OH 43216 | 614 614 | 236-2133 (Duty Hrs.) 236-2058 (After Hrs.) | 851-2133 |
| Richmond, VA | Director, DSI, c/o DGSC Richmond, VA 23297 | 804 | 275-4891 | 695-4891 |
| Brussels, Belgium | Mailing Address: Director, OISI APO New York 09667 Physical Address: Director, OISI Steenweg OpLeuven 13, 1940 St. Stevens-Woluwe, Brussels, Belgium | | 0-322-720-8259 | |
| Mannheim, Germany | Chief, OISI Field Office Hammonds Barracks, APO, NY 09333 | | (49621) 472582 | 380-8363 |
| Yokohama, Japan | Mailing Address: Chief, OISI-FE/V0470 DIS, MTMCTY, FPO Seattle 98760 Physical Address: Room 211 and 213, Bldg. 200, North Dock, Yokohama, Japan | | 045-441-0378 | 235-6703 |

**APPENDIX C. INDUSTRIAL SECURITY FUNCTIONAL RESPONSIBILITIES OF A
CONTRACTING OFFICER**

The following chart identifies some of the primary industrial security functional responsibilities of contracting officers. Some of these responsibilities shift from the PCO to the ACO after the contract award. A distinction has been made between related functions when performed on prime contracts and subcontracts. Paragraphs 1-101c(3) and 1-101d establish the general concept and outline broad responsibilities of contracting officers. Individual functional responsibilities are set forth under subject headings throughout this regulation and the ISM.

In addition to assigned functions, the ACO performs additional functions, delegated by the PCO, in accordance with guidance provided.

During contract performance, the ACO ensures that all functions assigned to him or her are accomplished and refers all other actions to the PCO for additional guidance or resolution, as required. During postcontract performance, the residual industrial security function reverts to the PCO.

INDUSTRIAL SECURITY FUNCTIONAL RESPONSIBILITIES OF A CONTRACTING OFFICER

| Function | PCO | Remarks | ACO | Remarks |
|---|-----|-------------------------|-----|---|
| 1. Provides special contract security requirements. (In addition to those in ISM.) | X | | | Prime Contractor includes in subcontracts. |
| 2. Establishes security classification by DD Form 254. | X | Original Classification | | |
| a. Reviews and signs DD Form 254. | X | For Prime | X | For Subcontractors |
| b. Reviews contract for reclassification as appropriate. | X | For Prime | X | For Subcontractors |
| c. Issues notice on review of classification. | X | For Prime | X | For Subcontractors |
| d. Gets resolution for any problem relating to classification. | X | Preaward | X | Postaward with referral to PCO when necessary |
| 3. Indicates on DD Form 254 the routing to the Directorate for Security Review, OSD, of contractor requests for public release of information pertaining to classified contracts. | X | For Prime | X | For Subcontractor |
| 4. Initiates request for FCL action. | X | For Prime | X | Prime contractor requests for prospective subcontractors. |
| 5. Furnishes justification for interim FCL | X | For Prime | X | For Subcontractors |
| 6. Authorizes release of classified information by contractors at seminars, meetings, and symposia, when authorization required. | X | Preaward | X | Postaward (refers to PCO when necessary) |
| 7. Reviews and furnishes written authorization for publication and distribution of classified sales literature. | X | Preaward | X | Postaward with referral to PCO when necessary |
| 8. Advises CSO and DTIC upon completion or termination of classified contract. | | | X | |
| 9. Advises contractor of method of shipment of classified material when required. | X | Preaward | X | Postaward (delegated to transportation element) |
| 10. Authorizes retention of classified material by contractor. | X | | X | Postaward, refers requests to PCO |

INDUSTRIAL SECURITY FUNCTIONAL RESPONSIBILITIES OF A CONTRACTING OFFICER (continued)

| Function | PCO | Remarks | ACO | Remarks |
|---|--------|--|--------|--|
| 11. Authorizes classified visits: a. Outgoing b. Incoming | X X | Preaward Preaward | X X | Postaward Postaward |
| 12. Approves expenditures of funds for security requirements; that includes, area controls, storage equipment, and protective alarms systems. | X | Preaward | X | Postaward with referral to PCO when necessary |
| 13. Reviews reports of security violations and recommends appropriate action. | X | Preaward | X | Postaward with referral to PCO when necessary (for example, compromises, and contract sanctions) |
| 14. Approves use of secure electrical transmission systems. | X | Coordinates with Military Department COR | X | Postaward, ACO would refer request to PCO with recommendation. |
| 15. Approves need for COMSEC material for R&D, production, installation, and maintenance. | X | Preaward Coordinates with Central office of Record and NASA, when appropriate | X | Postaward, ACO makes recommendation to PCO and COR. |
| 16. Appoints contractor employees as COMSEC material couriers (after contractor designates). | X | Preaward | X | Postaward |
| 17. Advise contractor of government representatives authorized access to controlled areas containing COMSEC material. | X | For PCO representatives | X | For ACO representatives |
| 18. Furnishes written approval to contractor to grant physical custody of TOP SECRET information to prospective subcontractors, vendors, and suppliers. | X | Preaward | X | Postaward |

In any instance where the ACO does not have sufficient knowledge to make a determination as required, he or she shall refer the matter to the PCO.

APPENDIX D. PREPARATION OF CLASSIFICATION GUIDANCE

D-100 Application. The following guidance is provided to assist those officials responsible for the preparation of the DD Form 254.

D-101 Determining Classification

a. Material is classified according to the classified information contained in or revealed by it. The development of the "DoD Contract Security Classification Specification" (DD Form 254) should be based on the concept that sensitive information itself shall be identified and assigned a proper classification rather than assigning a classification to the material by which classified information could be, or would likely be, conveyed. This method of classifying information rather than material is intended to identify most precisely the functional matter which is to be protected, thus providing the answer to the question, "What is there about an item which causes it to be classified?" Identification and knowledge of the precise information which requires classification will facilitate the application of classification to specific documents and material containing or revealing classified information, thereby reserving the security controls designed for safeguarding, disseminating, downgrading, and declassifying of information to only those documents and material which truly require security protection.

b. When considering the classifications to be assigned in a particular plan, program, project, or study, it is necessary to keep in mind the following fundamentals.

(1) It is information that is classified. A document, hardware, and other material is classified only by reason of the classified information which is contained in or on it, and can be revealed by observation, study, analysis, dismantling, operation, or use of it.

(2) To prevent unwitting or inadvertent disclosure of information which could or would prejudicially affect or negate the interests of national security, information should be considered for possible classification if it could reveal:

(a) derivative classified information;

(b) performance capabilities of the item which is responsible for or contributes to the U.S. advantage resulting from its possession or use;

(c) vulnerabilities, limitations, or weaknesses of the item which could be used to nullify or weaken its effectiveness, thereby causing loss of the U.S. advantages accruing from its possession or use;

(d) unique or peculiar designs, developments, or applications of materials, parts, processes, or techniques which are responsible for or contribute to the U.S. advantage resulting from its possession or use;

(e) U.S. military or defense capabilities which could be used to the disadvantage of the U.S. or to the advantage of any force which is or may be hostile;

(f) status, scope, or direction of U.S. research and development effort; or

(g) bases for, or direction, scope, or substance of U.S. military or defense planning or intelligence interest.

(3) Information is classified only if, through unauthorized disclosure, some harm or detriment could or would occur to national security. The threat must be more than a vague possibility but need not be immediate, readily measurable, or clearly predictable.

(4) Classification of identified information involved in the program, project, or activity may be required only if unauthorized disclosure could or would prejudice or damage the interests of national security by:

(a) providing any force which is or may be hostile to the U.S. with:

1 an insight into U.S. military offensive or defensive capabilities which could be used in planning or engaging in sanctions -- military, political, or economic -- or in acts of war or aggression against the U.S. or an ally;

2 a basis on which to develop a similar capability thereby minimizing or losing valuable lead time for the U.S. and the resulting advantage;

3 a basis for invoking or planning countermeasures or counteractions which could or would minimize or nullify the advantages accruing from the effort;

4 a basis for planning espionage or sabotage activities against the U.S. or an ally; or

5 useful strategic or tactical defensive or offensive data against the U.S. or an ally;

(b) causing loss of a valuable element of surprise or other U.S. advantage; or

(c) jeopardizing or harming U.S. foreign relations or commitments.

D-102 Suggested Method for Development of Guidance

a. Consider the end item to be obtained from the contract and write out the following, which itself will be a classified work document because it will reveal classified information pertaining to the end item.

(1) Decide why or how, not whether, the end item will or is expected to supply the U.S. with some kind of an advantage which, if disclosed to unauthorized persons, could or would cause harm to U.S. national security as indicated in paragraph D-101b(4) above.

(2) Explain the nature of the U.S. advantage, stated so as to show how the results obtained from use of the end item are involved (paragraph (1) above may be included so as to comprise one action).

(3) Explain why or how the end item will achieve or contribute to the attainment of that advantage.

(4) List the functions, uses, performance characteristics, or capabilities of the end item which will be responsible for or contribute to the successful attainment of that advantage (paragraph (3) above may be included so as to comprise one action).

(5) Indicate which of the elements listed under paragraph (4) above are critical, unique, or peculiar to the particular end item and to the results obtained from its use.

(6) Decide which of the items listed in paragraph (5) above will warrant classification. This decision will depend on findings that unauthorized disclosure of those items of information could or would result in some detriment of harm to U.S. national security under paragraph D-101b(4) above.

(7) The degree of resulting harm will determine the level of classification to be applied, that is TOP SECRET, SECRET, or CONFIDENTIAL, to each of the items of information listed under paragraph (6) above.

b. The next step is to determine as nearly as possible how the classified items of information are related or traceable to the elements of the contract, its performance, and the production of the end item. To accomplish this, the process described below is suggested. When worked out, this process may identify other related items of information requiring classification.

(1) If applicable to the type of program, project, or activity being covered, develop a "family tree;" that is, a chart or diagram showing the relationship of all separate identifiable elements of the end item to be realized from the contract. This "family tree" should depict those elements which have particular identified functions or operational uses, aligned to show operational sequence and relationships.

(2) Determine which items in the "family tree" are unique or peculiar to the particular end item or constitute new or unusual applications of ordinary parts or materials. (These are most likely subjects for possible classification.)

(3) Decide which items identified under paragraph (2) above contribute to or are responsible for the successful attainment of the functions, characteristics, performance, or capabilities of the end item which have been found to be classifiable under paragraph a(6) above, and in what way or how.

(4) Determine how the classified information under paragraph a above could or would be revealed by the items identified under paragraph (2) above and apply the considerations stated in paragraph D-101b(2) above.

(5) Determine whether and how any of the functions, uses, performance characteristics, or capabilities of any of the items listed under paragraph (2) above in themselves may require classification under the considerations stated in paragraph (4) above.

(6) Decisions under paragraphs (4) and (5) above will constitute the ultimate classification to be applied to information pertaining to the individual items in the "family tree" and to the items themselves.

c. The classification specification included with the DD Form 254 should consist of a series of unclassified meaningful statements identifying clearly and precisely the items of information which have been determined under paragraphs a and b above to be classified. These statements should be written so as not to reveal classified information. If an appropriate unclassified classification specification cannot be written, a classified specification should be issued under a separate cover as a supplement to the unclassified DD Form 254. When possible, determinations should be made and translated into meaningful language to show which parts of the elements listed in the "family tree" prepared under paragraph b(1) above require classification because they reveal information determined to be classified under paragraphs a and b above.

**APPENDIX E. AREAS SERVICED BY MTMC AND BY MILITARY COMMANDERS IN
ALASKA, HAWAII, PUERTO RICO, AND U.S. POSSESSIONS AND TRUST
TERRITORIES**

**AREAS COVERED BY MTMC AND THE MILITARY COMMANDERS IN ALASKA, HAWAII,
PUERTO RICO, AND A U.S. POSSESSION OR TRUST TERRITORY**

E-100 MTMC. Information and routing involving commercial carriers for the movement of SECRET controlled shipments within the CONUS may be obtained from MTMC area headquarters in the following defined regional areas:

a. Eastern Area

Telephone No.

Areas

Commander
Military Traffic
Management Command
Eastern Area
ATTN: MTE-IN
Bayonne, NJ 07002

Commercial:
201-858-6566

AUTOVON: 247-6566

Emergency Hotline:
800-524-0331
(New Jersey only:
201-823-5323)

Alabama, Arkansas, Connecticut, Delaware, District of Columbia, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, New Hampshire, New Jersey, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Vermont, Virginia, West Virginia, and Wisconsin.

*
*
*
*

b. Western Area

Commander
Military Traffic
Management Command
Western Area
ATTN: MTW-IN
Oakland Army Base
Oakland, CA 94626

Commercial:
415-466-3413

AUTOVON: 864-3413

Arizona, California, Colorado, Idaho, Montana, Nebraska, Nevada, New Mexico, North Dakota, Oregon, South Dakota, Utah, Washington, and Wyoming.

E-101 Designated Military Commanders. Information and routing involving commercial carriers for the movement of SECRET controlled shipments wholly within Alaska, Hawaii, Puerto Rico, or a U.S. possession or trust territory may be obtained from the following designated military commanders for their respective designated areas of responsibility.

a. Alaska
Address

b. Hawaii
Address

c. U.S. Possessions
and Trust Territories
Pacific Island
Address

d. Puerto Rico
Address

CDR 172d Inf Bde
(AK)
ATTN: AFZT-DI-T
Fort Richardson,
Alaska 99505

CDRUSASCH

CINCPACFLT

Commander
U.S. Army Garrison
AFZL-DIT
Fort Buchanan,
Puerto Rico 00934

APPENDIX F. FUNCTIONAL RESPONSIBILITIES OF MTMC, TO, AND CSO

The following chart identifies some of the primary functional responsibilities of MTMC, TO, and CSO with relation to transportation of SECRET controlled shipments by commercial carriers. Those functional responsibilities charged to MTMC are related to the CONUS. If the field of operation is in Alaska, Hawaii, Puerto Rico, or U.S. possessions or trust territories, those responsibilities charged to MTMC are to be performed by the responsible military Commander designated in appendix E.

FUNCTIONAL RESPONSIBILITIES OF MTMC, TO, and CSO

| No. | Function | (See Note 1) | | | Remarks |
|-----|--|--------------|----|-----|---|
| | | MTMC | TO | CSO | |
| 1. | Establishes need for a carrier (in coordination with contractor) and requests MTMC to qualify carrier. | | X | | |
| 2. | Determines if qualified carrier is available to perform required service. | X | | | MTMC shall coordinate this function with the Deputy Director (Industrial Security), HQ DIS to ensure that a cleared carrier is not available. |
| 3. | If qualified carrier is required and not available, proceeds to qualify a new carrier (that is, determines if carrier is authorized to perform the required services and that the carrier provides a PSS). | X | | | |
| 4. | Requests Deputy Director (Industrial Security), HQ DIS to authorize carrier to transport SECRET controlled shipments. | X | | | This action constitutes the request to clear a carrier at the SECRET level. |
| 5. | Executes a "Department of Defense Transportation Security Agreement" with the carrier and processes carrier for a SECRET PCL. | | | X | The CSO having jurisdiction of the geographical area where the HOF of the carrier is located. |

FUNCTIONAL RESPONSIBILITIES OF MTMC, TO, and CSO
(continued)

| No. | Function | (see Note 1) | | | Remarks |
|-----|--|--------------|----|-----|---|
| | | MTMC | TO | CSO | |
| 6. | Processes carrier terminals for SECRET FCL's. | | | X | |
| 7. | Inspects cleared carrier terminals used for SECRET controlled shipments. | | | X | |
| 8. | Maintains current records of approved carriers and the terminals used for SECRET controlled shipments. | X | | X | Close coordination is required to be effective. The CSO is the one having responsibility for the HOF. |
| 9. | Requests routing instructions for SECRET controlled shipments. | | X | | |
| 10. | Furnishes routing instructions for SECRET controlled shipments. | X | | | |
| 11. | Reports mishandling of SECRET controlled shipments to MTMC and CSO. | | X | | This report is in addition to those required from carriers, consignors, or consignees. |
| 12. | Assures the BL specifies, "Protective Security Service required," and is properly annotated regarding use of government seals. | | X | | |

NOTES:

1. The TO, rather than the contracting officer, is so designated on this chart to conform with "Remarks" for item 9, appendix C.

2. The above chart pertains only to SECRET controlled shipments. CONFIDENTIAL shipments may be made via cleared or uncleared commercial carriers in accordance with shipping instructions furnished by the TO.

Appendix G. FORMATS NECESSARY FOR NATO HAND-CARRIED MATERIALS *

The following three articles are to be completed by the CSO on official letterhead for each approved transport of hand-carried material by cleared contractor personnel. The formats include the Courier's Briefing Receipt, Courier Certificate in English and French, and details of the itinerary for the trip. Procedures for NATO hand-carried materials are found in section VIII of this regulation and section XI, DoD 5220.22-M. Each CSO shall maintain a record of the use of Courier Certificates. *

COURIER'S BRIEFING RECEIPT

(For personnel carriage within the U.S., omit inapplicable instructions.)

It has been found necessary to appoint you as an official courier to carry NATO classified material. Your courier authorization will accord the material you are carrying immunity from search or examination by customs and immigration officials of the countries whose borders you cross.

Attached are the security clearance certificates which you must have in connection with your forthcoming journey. You are reminded of the following precautions which you will observe for the protection of the classified material that you will carry.

1. The packages or bags containing the classified material must be covered by an official seal to prevent a customs examination.
2. A list of all NATO classified documents you will carry must be inventoried and recorded by the appropriate office of your department, agency, or command prior to your departure.
3. Throughout the journey and while at your destination, the classified material must never leave your possession unless deposited in a place of safety, as provided for under the security arrangements of the diplomatic or military missions or commands of this country, a national ministry of the host country, or with a NATO international agency.
4. NATO classified material must not be discussed in public places, such as hotels or lounges.
5. NATO classified material must not be read in aircraft, trains, ships, or any other vehicles.
6. NATO classified material must not be left unattended in hotel rooms, staterooms on trains or ships, or stored in repositories, such as hotel safes. You may delegate your responsibility for direct surveillance of the classified material you are carrying only under the security arrangements of a United States diplomatic mission, United States military command, a host NATO government, or a NATO international agency.
7. On your return, the classified documents (or receipts for them, if they were delivered into the custody of another authorized recipient) must be inventoried against the list prepared before your departure. Should any NATO classified documents be acquired, the COSMIC control officer, or other designated officer of your department, agency, or command will pick up accountability.

Some of the measures necessary to sustain good security may be cumbersome, especially when at the end of a tiring day's work a journey to some other part of the city is necessary in order to deposit your papers in a place of safety. It is easy to persuade oneself that no harm will be done by keeping the papers

overnight in the hotel or some equally insecure place. In reality, a person is presenting an easy target for the agents of foreign intelligence services by doing so, and the records of the security services of NATO countries contain cases of loss or compromise of documents attributable to this dangerous practice.

Should you encounter any security difficulties during your trip, please bring them to the attention of this office so that remedies may be worked out for the benefit of other NATO travelers.

Signature of appropriate briefing official

Date

I certify that I have read and understand the instructions set forth above which pertain to the handling of NATO classified documents in my custody while I am an official courier.

(Signature)

COURIER CERTIFICATE

Valid Until _____

1. This is to certify that the bearer _____ (name and rank, where applicable) _____, holder of Passport/Identity Card No. _____ is a member of _____ (parent organization) _____.

2. On the journeys detailed overleaf, the bearer is travelling in the execution of his official functions and is designated as an official NATO courier. He is authorized to carry _____ (number) _____ of packages of official NATO documents, the seals on which correspond to the specimen seal appearing against the appropriate journey.

3. All customs and immigration officials concerned are, therefore, requested to extend to the official correspondence and documents being carried under official seal by the bearer the immunity from search or examination conferred by the Agreement on the Status of the North Atlantic Treaty Organization National Representatives and International Staff, and the Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces.

Signature of Authorizing Official:

Designation:
(Name and rank in capitals)

Date:

Official stamp of NATO member
nation or NATO command or agency.

COURIER CERTIFICATE, continued:

ORDRE DE MISSION D'UN COURRIER

Valable jusqu'au _____

1. Il est certifié par la présente que le porteur (nom et grade,
le cas échéant), détenteur du Passeport/Carte d'identité
No. _____ est membre de _____ (organisme d'appartenance)

2. Au cours des voyages mentionnés au verso, le porteur voyage en exécution de ses fonctions officielles et est accrédité comme un courrier officiel de l'OTAN. Il est autorisé à transporter (nombre) paquets contenant des documents officiels de l'OTAN, dont les sceaux correspondent au modèle du sceau apposé en regard du voyage indiqué.

3. Tous les fonctionnaires des services de douanes et de l'immigration sont, en conséquence, priés d'appliquer à la correspondance et aux documents officiels transportés sous sceau officiel par le porteur l'immunité prévue en matière de visite et de contrôle douanier par la Convention sur le Statut de l'Organisation du Traité de l'Atlantique Nord, des Représentants nationaux et du Personnel international et la Convention entre les Etats parties au Traité de l'Atlantique Nord sur le Statut de leurs Forces.

Signature du fonctionnaire responsable:

Designation:
(Nom et grade en majuscules)

Date:

**Sceau officiel du pays membre
de l'OTAN ou du commandement
ou organisme de l'OTAN**

COURIER CERTIFICATE continued:

DETAILS OF ITINERARY
DETAILS DE L'ITINERAIRE

SPECIMEN OF SEAL USED
MODELE DU SCEAU UTILISE

From to
De 'a

See note below
Voir note ci-dessous

From to
De 'a

From to
De 'a

From to
De 'a

NOTE: In addition to an impression of the seal, the officer affixing the seal must print his name, rank, and the name and address of his department, command, agency or facility.

En complément à l'impression du sceau, le fonctionnaire apposant le sceau doit mentionner en majuscules, son nom et grade ainsi que le nom et l'adresse de son service, commandement, organisme ou établissement.

APPENDIX H. INDEXACDA, 1-101h, 2-117a(5)Assurances, Facility Security, 2-117Assurances, Individual, 2-322, 2-323Authority and Scope of Industrial Security Regulation, 1-101Board Resolutions, 2-205aBriefings and Debriefings, Defense Security:

COMSEC Access, 1-108b(13), 1-108a(7), 2-314

Contractor Activities on User Agency Installation, 1-108b(7), 1-108e(5)

Intelligence, 2-317

Type A Consultants, 1-304a

Visits by Designated Country Representatives, 1-304b

Carve-outs, 1-114f, 1-205.1 *Classification and Declassification:

Application and Procedures, 7-100

Classification Interpretation Procedures, 7-105

Downgrading and Declassification, 7-107

FOR OFFICIAL USE ONLY -- Protective Marking, 7-108

Issuance of Classification Guidance (DD Form 254), 7-102, 7-105:

Classification Review, 7-104a

COMSEC or Other Special Access Programs Contracts, 7-102g

Determining Classification, Appendix D-101

Development of Guidance, Suggested Method, Appendix D-102

Final, 7-102b

Need-to-Know Review, 7-104d

Notification of Review Results, 7-104c

Original, 7-102a

Public Disclosures, 1-113, 7-102i

Reference Material, 7-102e

Required Review (Distribution), 7-103

Review Not Required, When, 7-104b

Revised, 7-102c

Special Situations, 7-102d

Subcontract Guidance, 7-102f

Unsolicited Proposals, 7-102h

Waivers to, 7-100h

Retention of Classified Material, 7-106

Security Classification, 7-101

Classification Guidance (See Classification and Declassification), 7-102Classification Review, 7-104Classified Material Retention, 7-106

Clearances, Facility:

Administrative Termination, 2-119

Changed Conditions:

Address Change, 2-118c

Adverse Information Notification, 2-118j

Adverse Personnel Actions, 2-118e

Closing of Business, Bankruptcy, 2-118d

Debarred Bidders' List, 2-118g

FOCI Changes, 2-118k

General Procedures, 2-118

Operating Name Change, 2-118a

Ownership or Management Change, 2-118b

Parent Organization Changes, 2-118h

RFI Changes, 2-118f

Upgrading of Facility Clearance, 2-118i

Cognizant Security Office Responsibilities, 2-111a, 2-111b

Debarred Facilities, 2-111g, 2-118g, 2-122d

Definition of, 2-102a

Denial, Suspension, or Revocation of, 2-121, 2-122

Eligibility for Access, 2-101

Eligibility for Clearance, 2-102a

Facility Security Assurances, 2-117

Facility Under FOCI, 2-102a

FOCI (See Foreign Ownership, Control, or Influence)

Granted by Cognizant Security Office, 1-101c(1)

Ineligible OODEP, 2-111d

Initial Survey, 1-108d, 2-103, 2-116d

Interim Clearances, 2-102b, 2-111b

NAC, 2-110, 2-111c

OODEP Clearances:

Colleges and Universities, 2-113d

Commercial Carriers, 2-113e

Corporations, Associations, and Nonprofit Organizations, 2-113a

Eligibility Determinations, 2-113f

Exclusion Procedures, 2-113g

Foreign National OODEPs, 2-114

Negotiators (See Clearances, Personnel)

Partnerships, 2-113c

RFIs, 2-113h

Sole Proprietorships, 2-113b

Procedures for Processing:

Assumption of Security Cognizance, 2-116b

Certificate Pertaining to Foreign Interests, 2-104b(2), 2-116e(3), 2-116f

DoD Technical Information Dissemination Activities, 2-116j

Documents Forwarded to DISCO, 2-116g

Final Actions, 2-116i

Follow-up Action, 2-116h

Initial Visit, 2-116c

Justification, 2-116a

Reciprocal, 2-116j(3)

Security Agreement, 2-116a(1)

Security Agreement Appendage, 2-116a(2)

Security Survey, 2-116d

Processing Responsibility, 2-103

Reprocessing or Revalidation of, 2-120, 2-123

Restricted Data, 2-112
 SPP Requirement, 2-111h
 Termination, Revocation, or Suspension of Facility Clearance, 1-108b(12),
 1-108c(4)
 TOP SECRET Facility Clearances, 2-111e, 2-111i
 Types of Facilities:
 Commercial Carriers, 2-104g
 Commercial Messenger Service, 2-104h
 Consultants, 2-105
 Multiple Facility Organization, 2-104a
 Parent Facilities, 2-104c
 Parent-Subsidiary Relationships, 2-104b
 Single Facility Clearances, 2-104d
 Small Business Pools, 2-104e
 Temporary Help Suppliers, 2-104f
 Upgrading, 2-111f
 Verification of Clearance and Storage Capability, 1-108c(3), 1-110, *
 1-111b, 1-111.1, 1-409, 2-118j *

Clearances, Personnel

Access to NATO Classified Information, 2-321
 Administrative Downgrading of TOP SECRET, 2-311
 Administrative Termination of, 2-301d, 2-310
 Application, 2-300
 Colleges and University Personnel, 2-318
 COMSEC Requirements:
 Briefing and Debriefing, 2-314, 1-108
 Clearance Processing, 2-313
 Conversion of Clearances:
 DOE and NRC Clearances, 2-309b, 2-309c
 Executive Branch Clearances, 2-309a
 Critical Nuclear Weapon Design Information (CNWDI) Requirements, 2-212.1
 DISCO, 2-302
 Denial of Admittance to User Agency Installations, 2-316
 Denial, Suspension, or Revocation, of, 2-320
 General Procedures, 2-301a
 Granted by DISCO, 1-101b(2)
 Hostage Case Processing, 2-305
 Immigrant Aliens, 2-307h, 2-327
 Intelligence Briefing and Debriefing, 2-317
 Interim Personnel Clearances, 1-108b(10), 1-108e(10), 2-301b
 Invalid and Void Clearances, 2-301c
 Negotiators, 2-115
 PRP Requirements, 2-324
 Requirements for Processing:
 CONFIDENTIAL, 2-308f
 Interim CONFIDENTIAL, 2-308g
 Interim SECRET, 2-308e
 Interim TOP SECRET, 2-308c
 Prior DoD Investigations, 2-308h
 SECRET, 2-308d
 TOP SECRET, 2-308b
 Responsibility for Effecting, 2-307

RESTRICTED DATA, 2-312

RFI Processing, 2-306

Security Assurances:

Nationals of Signatory Governments, 2-323

U.S. Citizens (Bilateral Reciprocal), 2-322

SENSITIVE COMPARTMENTED INFORMATION Requirements, 2-315

Special Status of Certain Canadian Born American Indians, 2-303

Transfer of MFO Personnel, 2-304

Types of Personnel Investigations:

Background Investigations, 2-319b

Other Investigations, 2-319c

Personnel NAC, 2-319a

User Agency Reporting Adverse Information, 2-319.1

Closed or Restricted Areas, 1-108b(9)

"Close-Out" Inspections, 4-300

Cognizant Security Office Responsibilities, 1-103b

OOEPS, Processing of, 1-103d

Security Actions Performed by Head of Installation, Relative to:

Grant Facility Clearance, 1-108c(1)

Inspections, 1-108c(2)

Terminate, Revoke, Suspend Facility Clearance, 1-108c(4)

Verify Facility Clearance and Safeguard Ability, 1-108c(3)

Commercial Carriers

Approval of, 1-702

Authority for Security Cognizance, 1-300f

Central Master File, 1-300h

Escorts, 1-300g

Facility Clearance Requirements, 2-104g, 2-113e

Glossary of Terms, Annex A of DoD 5220.22-C

Inspection Report, 4-106

MTMC, Areas Serviced, appendix E

MTMC, Functional Responsibilities, appendix F

Protective Services Provided, 1-702b

Qualifications, 1-702a

Responsibilities of Cognizant Security Office, 1-703

Security Procedures, 1-101f

Shipment by Truck, 1-300g

COMSEC

Application Procedures and Conditions, 1-500

Briefings, 1-108b(13), 1-108e(7), 2-313

Clearance Requirements, 2-313 and 2-314

Destruction and Disposition, 1-505

Establishing a COMSEC Account, 1-504

Inspections, 4-107

NSA Operational Responsibility, 1-306

Release to U.S. Contractors, 1-502

Requirements, 1-501

Shipment, 1-506

Subcontracting COMSEC Work, 1-503
Unsolicited Proposals, 1-507

Consultants

Classified Material, Transmitted To, 1-601c
Disclosure of CNWDI, 1-111.1c
Employed Under Civil Service Procedures, 2-109
Type A, 2-106
Type B, 2-107
Type C, 2-108

Contracting Officer, Industrial Security Functional Responsibilities, appendix C

Contractor Activities Located On User Agency Installation, 1-103b, 1-108

Contracts Performed Abroad, 1-115

DISCO Responsibilities, 1-115b
Security Cognizance, 1-115a
User Agency Responsibilities, 1-115c

Conversion of Clearances, 2-309

CNWDI

Disclosure of, 1-111.1
Requirements for Access, 2-312.1

Critical Technology, 1-221.2

*

Debarred Facilities, 2-111g, 2-118g, 2-122d

DISCO:

Clearance Responsibility, 1-300e, 2-302
Contracts Performed Abroad, 1-115b
Files, 2-403
Foreign Travel, 1-304a(1)
Personnel Clearances, 2-307
Responsibilities, 1-101c(2), 1-103d, 2-302
Type A Consultant, 1-304a
Verification of Personnel Security Clearances, 2-404

DIS Operational Areas, appendix B

Definitions, 1-200

Denial, Suspension, or Revocation of Facility Clearances, 2-121, 2-122

Designated Countries (list of), 1-304a

DOE and DoD Programs (Reciprocal Use), 4-102

Downgrading and Declassification, 7-107

Emergency Safeguard Procedures, 1-101d

Essential Elements of Friendly Information (EEFI), 1-227.1

Facilities, Types of, 2-104

Facility, Changed Conditions, 2-118

Facility Files, Maintenance of:

- Application, 2-400
- Cognizant Security Office Responsibilities, 2-402
- DISCO Responsibilities, 2-403
- File Folders, 2-401
- Verification of Personnel Security Clearances, 2-404

Foreign Classified Contracts or Subcontracts in the U.S., 8-103

Foreign Classified Information, Access to, 8-500

Foreign Classified Information, Safeguarding of, 8-102

Foreign Nationals:

- Meetings Attended By, 1-407
- OODEPs, 2-114

Foreign Ownership, Control, or Influence:

- Annual Visit to Excluded Parent, 2-104b(2)(d)
- Appeals, 2-203e
- Assistance by Cognizant Security Office, 2-204
- Certification, 2-207
- Changes Affecting Facility Clearance, 2-118k
- Criteria for Determination, 2-202
- Effects On Prior Clearances, 2-208
- Facilities Under FOCI, 2-102a
- General Policy, 2-201
- Method To Remove or Negate Effects of:
 - Board Resolution, 2-205a
 - Proxy Agreement, 2-205c
 - Special Security Agreement, 2-205e
 - Voting Trust Agreement, 2-205b
- Processing Procedures, 2-203
- Visitation Agreements, 2-206

Foreign Travel, 1-304

Forms, Industrial Security:

- Exhibit of Forms, part 2, section 9
- Index of Forms, 9-100

FOR OFFICIAL USE ONLY -- Protective Marking, 7-108

Functional Responsibilities of MTMC, TO, and CSO, appendix F

Glossary of Acronyms and Abbreviations, pages vii, viii, ix, and x

Hostage Case Processing, 2-305

Immigrant Aliens:

Contracting Officer Responsibilities, 2-327
 Personnel Clearance Processing, 2-307h
 Visits, 3-104a(2)

Independent Research and Development, 1-101c(1)Inspection Reports:

Exchange with Head of User Agency Installation, 1-108d
 Use of, 4-105

Inspections, Security:

By Contractor on User Agency Installation, 1-108e(3)
 "Close-out" Inspections, 4-300
 Commercial Carrier Inspection Report (DIS Form 1148), Use of, 4-106
 COMSEC Inspections, 4-107
 DOE and DoD Programs (Reciprocal Use), 4-102
 Exchange of Inspection Reports, 1-108d
 Formal Notification of Results, 4-108
 Frequency of, 1-103d
 Inspection Report (DD Form 696), Use of, 4-105
 Notification of Inspection, 4-104
 OPSEC, 4-103h, 10-104
 Purpose, 4-101
 Remedial Action By Head of User Agency Installation, 1-108e(4)
 Schedule, 4-103
 Tempest Countermeasures, 4-105.1
 Unsatisfactory Inspections:
 Commercial Carrier, 4-202
 Procedures, 4-201

*

Interim Clearances, Facility, 2-102b, 2-111bInterim Clearances, Personnel, 1-108b(10), 1-108e(10), 2-301bInternational Security Programs:

Access to Classified Information of Foreign Governments:
 Administrative Termination, Letter of Consent, 8-502
 Annotation of Clearance Records, 8-503
 General Information, 8-500
 Security Assurance, 8-501
 Application of Procedures, 8-104, 8-200, 8-202
 Foreign Classified Contracts or Subcontracts in the U.S.:
 Channels of Transmission, 8-102g
 Cognizant Security Office Responsibilities, 8-103d
 Deputy Director (Industrial Security), HQ DIS, Responsibilities, 8-103c
 Loss or Compromise, 8-103d(4)
 Preliminary Contracts, 8-103a
 Received from Outside U.S., 8-102g(2)
 Table of Functional Responsibilities, 8-103
 Transmitted Outside U.S., 8-102g(1), Appendix G
 General, 8-102:
 Costs, 8-102a
 Security Requirements Clause, 8-102f
 Subcontracts, 8-102e

Transmission of Classified Material, 8-102b
"U.S. Munitions List" Items, 8-102d
Use of U.S. Information, 8-102c
Overseas Operations of U.S. Contractors:
Access, 8-401
General Information, 8-400
Safeguarding U.S. Classified Information:
Custody and Storage, 8-402b
Disclosure, 8-402c
Transmission, 8-402a, Appendix g
U.S. Classified Contracts, Awarded to Foreign Contractor, 8-104
U.S. Patent Agents (For Foreign Governments):
Application, 8-200
General, 8-201
Participating Countries, 8-203
Procedures, 8-202

Interpretations, Request For, 1-303

Invalid and Void Clearances, 2-301c

MTMC:

Areas Serviced, appendix E
Functional Responsibilities, 1-101h, 1-103e, appendix F

NAC, 2-110, 2-111c

NATO:

Access to, 2-321
Hand-carried Material 1-603
Visit Procedures, 3-501

NPLO Visit Procedures, 3-502

Negotiators, 2-115

Notification of Security Assignment, 1-302

Objective of the Industrial Security Program, 1-100

OISI:

Activities on User Agency Installation, 1-108f
Addresses, 8-302
Functions, 8-301
General Information, 8-300

Overseas Operation of U.S. Contractors, 8-400

ODEPs:

Clearances, 2-113
Foreign Nationals, 2-114
Ineligible, 2-111d
Processing by Cognizant Security Office, 1-103d

Operations Security (OPSEC):

Application, 10-102
 Authorization and Scope, 1-101d
 Definition, 1-252a
 General, 10-101
 OPSEC Indicators, 1-252b
 Procedures for Inspecting, 4-103h, 10-104
 Purpose, 10-100
 Responsibilities, 10-103

*
*
*
*
*
*
*
*

Patent Agents, 8-200Privileged Information, 1-116Processing, Facility Clearances (See "Clearances, Facility")Processing, Personnel Clearances (See "Clearances, Personnel")Proxy Agreement, 2-205cPublic Disclosures, 1-113, 7-1021References, pages v and viRelease of Economic and Technical Information, appendix AReprocessing or Revalidation of Facility Clearances, 2-120, 2-123Representatives of a Foreign Interest:

Changed Conditions, 2-118f
 Clearance Processing, OODEP, 2-113h
 Clearance Processing, Personnel, 2-306
 Meetings, Attendance by, 1-407

Restricted Data, 2-112Scientific and Technical Information Release Program, 1-110eSecurity Assurances, 2-117, 2-322, 2-323Security Costs, 1-109Security Education:

Application, 6-100
 Distribution of Material, 6-105
 Funding, 6-103
 Material Available, 6-104
 Preparation of Material, 6-102
 Responsibilities, 6-101
 Training Schools, 6-106
 User Agency Installation, By Head Of, 1-108e(5)

SENSITIVE COMPARTMENTED INFORMATION:

Access Authorization Processing, 1-305d

Contracts Awarded By:

NSA, 1-305a

Other User Agencies, 1-305b

Contract Security Classification Specification, 1-305c

Requirements, 2-315

Special Access Programs:

Additional Investigative Requirements, 1-114e

Authority to Establish, 1-114b

Authorization for Access, 1-114d

Carve-out, 1-114f

COMSEC or Other Special Access Contracts, 7-102g

Incorporation in Contracts, 1-114c

Sponsorship of Meetings:

Approval for Attendance at Classified Meetings, 1-409

Attendance by Foreign Nationals and RFIs, 1-407

Controlling Disclosures, 1-406

Disclosure Authorizations, 1-408

General Policy, 1-401

Guides for Sponsorship, 1-403

Location of Meetings, 1-404

Notification of Meetings, 1-410

Requests for Sponsorship, 1-402

Security Procedures, 1-405

Types of Meetings, 1-400

SPP, 1-108b(2), 2-111h

Summary of Changes, pages iii and iv

Survey, Facility Security, 1-108d, 2-103, 2-116d

Tempest Countermeasures, 4-105.1

Termination of Personnel Clearances, Administrative, 2-301d, 2-310

Termination, Revocation, or Suspension of Facility Clearances, 1-108b(12), 1-108c(4)

Training Schools, 6-106

Transmission of Classified Material:

Application, 1-600

Approved Methods, 1-601

Classified Hardware, 1-601d

Hand-carrying Aboard Commercial Aircraft, 1-601e

NATO, 1-603

Requiring Contracting Officer Approval, 1-602

Shipment of SECRET Material, 1-103e

U.S. Express Mail, 1-601

Unsatisfactory Inspections, 4-201, 4-202

Unsolicited Proposals, 7-102h

User Agency Procedures, 1-107

Verification of Clearance and Storage Capability, 1-108c(3), 1-110, 1-111b, *
1-111.1, 1-409, 2-118j *

Violations, Security:

Additional Reporting Requirements, 5-104
Contractor Activities on User Agency Installation, 1-108b(11), 1-108e(11)
Espionage, Sabotage, and Subversive Activities, 5-101
Inquiries into Delays, Tampering, or Improper Shipping Methods, 5-108
Investigation by Contracting User Agency, 5-107
Investigation by Head of User Agency, 1-108b(8), 1-108e(6)
Investigative Support, 5-103
Loss, Compromise, and Suspected Compromise, 5-102
Other Administrative Violations, 5-106
Other Security Violations, 5-105

Visits:

By Communist Country Representatives, 1-304b
By User Agency, 1-300c
Visits to Foreign Governments and Activities:
Application, 3-400
ITAR Guidance, 3-400b
Processing Time, 3-400f
Visits to Government Activities Other Than User Agencies:
DOE Installation or DOE Contractors, 3-301
Other Visits, 3-302
Visits to User Agency Activities:
Compliance With User Agency Request, 3-205
General Rules, 3-201
Outside the U.S., 3-203
User Agency Actions, 3-204
Within the U.S., 3-202
Visits to User Agency Contractors:
East-West Visit Exchange Program, 3-106
General Rules, 3-101
Investigative Requirements, 3-104a
Long-Term Visits, 3-102
RESTRICTED DATA, Visits Involving Access to, 3-105
Visitor Categories and Procedures:
Category 1, 3-103a
Category 2, 3-103b
Category 3, 3-103c
Category 4, 3-103d
Category 5, 3-103e

Voting Trust Agreement, 2-205b

Waivers and Exceptions to the Industrial Security Regulation, 1-114a