12 FAM 570 INDUSTRIAL SECURITY PROGRAM

12 FAM 571 SCOPE AND APPLICABILITY

12 FAM 571.1 Scope

(TL:DS-40; 10-12-94)

a. The Bureau of Diplomatic Security, Office of Information Security Technology, Information Security Programs Division, Industrial Security Branch (DS/ISP/INB), administers the Department's Industrial Security Program. DS/ISP/INB establishes policies and implements procedures to ensure the appropriate safeguarding of classified and sensitive unclassified information which is released to or generated by prime contractors, subcontractors or self-employed individuals under contract to the Department. This includes all private sector individuals supporting Department activities either assigned at DOS locations or performing on contracts from their companies' respective physical locations.

b. These regulations and procedures apply to firms and/or individuals performing under contract to the Department from pre-contract award to post-contract completion. In the case of private sector individuals who support Department activities but are not under contract, these regulations apply from the beginning of the support period through completion of the activity. All Department contract actions must comply with the Federal Acquisition Regulation (FAR) and Department of State Acquisition Regulation (DOSAR) (see 6 FAM, *General Services*). The FAR and the DOSAR take precedence if any conflicting interpretations result from this subchapter.

12 FAM 571.2 Applicability

(TL:DS-40; 10-12-94)

These regulations and procedures apply to the Department's domestic and overseas operations, including U.S. missions to international organizations.

12 FAM 571.3 National Industrial Security Program

(TL:DS-56; 2-20-97)

a. The Department of State, through DS/ISP/INB's Industrial Security Program, *participates in the National Industrial Security Program (NISP). The NISP was established by E.O. 12829 on January 6, 1993, for the protection of information classified pursuant to E.O. 12356, April 2, 1982, "National Security Information," or its successor or predecessor orders, and*

the Atomic Energy Act of 1954, as amended. The National Security Council is responsible for providing overall policy direction for the NISP. The President designated the Secretary of Defense as Executive Agent for the NISP. The Director, Information Security Oversight Office (ISOO), is responsible for implementing and monitoring the NISP and for issuing implementing directives that shall be binding on agencies.

b. Prior to the NISP, the Department formalized its use of the industrial security services of the Department of Defense as a user agency of the Defense Industrial Security Program by Memorandum of Agreement, dated June 5, 1961. The Department's continued participation in the NISP supplements its security resources and enhances oversight of classified activities by contractors.

c. The Defense Investigative Service (DIS) issues and maintains facility security clearances and personnel security clearances, as required, for Department of State contractors. DIS inspects and monitors contractors who require or will require access to classified information. The Defense Industrial Security Clearance Office (DISCO), a field element of DIS, issues personnel security clearances under the authority of the NISP. The standards for implementing the NISP are promulgated in DoD 5220.22-R and DoD 5220.22-M. They establish requirements for safeguarding classified information, including foreign government information, which the U.S. Government is obliged to protect in the interest of national security, and to which access may be required by contractors, subcontractors, vendors, or suppliers.

d. DS/ISP/INB:

(1) Issues State Department's industrial security policies and standards;

(2) Serves as liaison with the Department of Defense regarding the industrial security program; and

(3) Coordinates issues concerning contractor performance of Department contracts and compliance with security requirements.

12 FAM 571.4 Legal Authorities

(TL:DS-56; 2-20-97)

a. Executive Order 12958, Classified National Security Information, April 17, 1995, and succeeding orders which prescribe a uniform information security program.

b. Executive Order 10865, Safeguarding Classified Information Within Industry, February 20, 1960, as amended by Executive Order 10909,

December 7, 1966, and succeeding orders, which direct Federal agencies to establish regulations governing the handling and protection of its national security information by U.S. industry.

c. Executive Order 12829, National Industrial Security Program (NISP), *January 6, 1993,* provides for a uniform program for safeguarding Federal Government classified information that is released to contractors, licensees or grantees of U. S. Government Executive Branch departments and agencies.

d. The Omnibus Diplomatic Security and Antiterrorism Act of 1986, (Pub.L. 99-399) Section 403 (22 U.S.C. 4853), Security Requirements for Contractors, directs the Department of State to strengthen its Industrial Security Program for diplomatic construction projects.

e. DoD 5220.22-R, Industrial Security Regulation, current edition, sets forth the requirements of User Agencies in *the National Industrial Security Program*.

f. DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)* for Safeguarding Classified Information, current edition, prescribes the regulations industries must follow to safeguard national security information.

g. DoD 5220.22-M-Sup 1, National Industrial Security Program Operating Manual Supplement, current edition.

12 FAM 572 PROGRAM MANAGEMENT

(TL:DS-48; 9-28-95)

Department program, project and contracting personnel must consider security requirements at the earliest possible stage in the procurement process. The responsibility for effective implementation of the Department's Industrial Security Program must be shared by the:

(1) Bureau or office project manager;

(2) Contracting officer's representative (COR);

(3) Contracting officer;

(4) Unit security officer; and

(5) Bureau of Diplomatic Security (DS).

12 FAM 573 SECURITY CLEARANCE POLICY

(TL:DS-56; 2-20-97)

To ensure that classified information entrusted to the private sector is properly safeguarded, the Department requires that firms and individuals be processed for a security clearance. The *following* policies apply to clearing private sector personnel for access to classified information:

12 FAM 573.1 Firms

12 FAM 573.1-1 Facility Security Clearances (FCL)

(TL:DS-56; 2-20-97)

a. Any firm or business under contract to the Department which requires access to classified information will need a facility security clearance commensurate with the level of access required. Additionally, any firm or business entity which requires access to classified information to prepare a response to an RFP, IFB, etc., and/or in performance of a classified Department contract will require a facility clearance. Firms which do not possess a facility clearance, or the requisite level facility clearance, will be sponsored for a DOD facility clearance by DS/ISP/INB.

b. Department contracting authorities must submit facility clearance requirements and requests to DS/ISP/INB. A firm's employees will also be processed for clearances through DISCO. However, certain positions will require Department clearance, as outlined in 12 FAM 577 .

12 FAM 573.1-2 Joint Ventures

(TL:DS-48; 9-28-95)

A classified contract issued to a joint venture requires that those elements comprising the joint venture possess a facility clearance. DS/ISP/INB will process requests to clear those elements.

12 FAM 573.1-3 Reciprocal Facility Security Clearances

(TL:DS-56; 2-20-97)

Reciprocal facility clearances may be granted to foreign-owned U.S. firms based upon guidance contained in DOD 5220.22.M. They are not valid for access to certain types of classified information. In addition, the use of reciprocally cleared firms for classified procurements at some overseas posts is prohibited. DS will consider approving the use of reciprocally cleared firms on a case-by-case basis. The COR must submit justification for the use of reciprocally cleared firms to DS/ISP/INB for processing.

12 FAM 573.2 Individuals

12 FAM 573.2-1 Self-Employed Contractors

(TL:DS-56; 2-20-97)

The Department may hire self-employed individuals on a contractual basis. By definition, they must have no affiliation with a company or firm. Individuals incorporated for tax purposes who may have family members as office holders of the corporation would also qualify as self-employed contractors. Consultants or expert consultants hired through the Bureau of Personnel (PER) under Federal personnel regulations are not covered by this guidance. Self-employed contractors are either cleared by DISCO or DS. For the purpose of the industrial security program, self-employed contractors are also referred to as "consultants." Specific guidance is contained in 12 FAM 577 .

12 FAM 573.2-2 DOS Contractor Personnel

(TL:DS-48; 9-28-95)

Individuals employed by a firm will be cleared through DISCO. The cleared firm is required to have a designated facility security officer (FSO) through whom requests for personnel security clearances are submitted to DISCO. The FSO is also responsible for submitting visitor authorization requests (VARs) on all cleared employees to DS/ISP/INB.

12 FAM 573.3 Personnel Security Requirements

12 FAM 573.3-1 Domestic Personnel Security Requirements

(TL:DS-48; 9-28-95)

Contractor personnel must have clearances commensurate with the level of access required for performance under the Department contract.

12 FAM 573.3-2 Overseas Personnel Security Requirements

(TL:DS-56; 2-20-97)

DS has established clearance requirements for U.S. contractors performing under contract to the Department for the critical human intelligence threat posts as listed in the Department's composite threat list. These requirements are based upon the duration of the visit and area(s) to be accessed. *Definitions of these U.S. contractor clearance requirements follow below.*

A. Classified Projects on the Compound

(TL:DS-56; 2-20-97)

a. ***Classified contracts: Access to controlled access area (CAA)**:*

(1) ***Restricted areas, spaces contiguous to the controlled access area (CAA), and secure storage areas (assignment 0 - 60 days)****: Final Secret personnel security clearance (PCL), unless access to Top Secret classified information is required;*

(2) ***Restricted areas, spaces contiguous to the controlled access area (CAA), and secure storage areas (assignment more than 60 days)****: Final Top Secret personnel security clearance (PCL) or Secret PCL with appropriate background investigation, with DS acceptability review completed or pending;*

(3) ***Core areas (any length of assignment)****: Final Top Secret personnel security clearance (PCL) or Secret PCL with appropriate background investigation, with DS acceptability review completed or pending.*

NOTE: A contractor employee could be deployed before the DS acceptability review is completed. However, if the acceptability review is adjudicated unfavorably, the contractor employee must be immediately removed from the site upon notification by the COTR at no expense to the U.S. Government. The 60-day period is cumulative within one year.

b. ***Unclassified portions of classified contracts: Access to general work areas and/or public access areas****: Favorable national Agency check (NAC) (OPM, DCII, FBI, NCIC records checks) credit check; personal interview prior to deployment, if deemed necessary by DS. Form DS-1897, Access Authorization, must be issued¾no access to classified information authorized.*

B. All Other Unclassified Projects on or off the Chancery/Consulate Property

(TL:DS-56; 2-20-97)

Favorable NAC (OPM, DCII, FBI, NCIC records checks) credit check; personal interview prior to deployment, if deemed necessary by DS. Access Authorization, DS Form 1897, must be issued--no access to classified information authorized.

C. The Cleared American Personnel Program for the Bureau of European Affairs' Program Are Different from the Guidelines Provided in 12 FAM 573 Exhibit 573.3-2

(TL:DS-56; 2-20-97)

These individuals will ordinarily require a single-scope background investigation conducted by the Department of State. DS may accept Top Secret or equivalent clearances granted by other U.S. Government agencies upon receipt of investigative files which are reviewed and evaluated for acceptability for deployment to certain Department of State posts. DS may conduct further investigation as required.

12 FAM 573.3-3 Definitions

(TL:DS-56; 2-20-97)

a. ***Chancery/consulate****: High visibility facility with its own compound, containing highly classified and sensitive information or equipment, occupied by a large number and wide range of U.S. Government interests and activities. Includes office annex containing U.S. citizens on the same compound as the chancery or consulate.*

b. ***Contiguous area****: A buffer zone that shares a common boundary with a controlled access area.*

c. ***Contractor****: As used in this document, the term contractor means a U.S. personal services contractor serving under the authority of a chief of mission and contract employees under the authority of a commercial contract serving under the chief of mission.*

d. **Controlled access area (CAA)**: Controlled access areas are specifically designated areas within a building where classified information may be handled, stored, discussed, or processed.

e. ***Core****: Those areas of the building requiring the highest levels of protection where intelligence, cryptographic, security, and other particularly sensitive or compartmentalized information may be handled, stored, discussed, or processed.*

f. ***General work area****: Areas of the building in which sensitive but unclassified information may be handled, stored, discussed, or processed.*

g. ***Public access area****: Areas within the building where services are provided to the general public. There is no handling, storing, discussing, or processing of classified, controlled, or sensitive unclassified materials.*

h. **Restricted area**: Areas of the building in which classified information may be handled and stored. Classified discussions and processing are permitted but may be limited to designated areas, depending on the technical security threat.

i. ***Secure storage area****: A specially prepared secure room with floor-to-ceiling, slab-to-slab construction of some substantial material with a minimum solid wood core or steel clad door and equipped with an approved controlled security keyed deadbolt or integral changeable combination lock. Other alternatives may include: a secure shipping container located within a secure perimeter and continuously monitored by a cleared U.S. citizen employee; a room, or outside location enclosed by a secure perimeter, under direct observation of a cleared U.S. citizen employee; or within the PCC on a case-by-case basis.*

12 FAM 573.4 Special Program Requirements

12 FAM 573.4-1 Special Access Programs (SAPs)

(TL:DS-56; 2-20-97)

The Department program office, in coordination with DS/ISP/INB, determines contractor clearance requirements for special access programs. *They will be processed in accordance with the NISPOM Supplement.*

12 FAM 573.4-2 SCI Requirements

(TL:DS-56; 2-20-97)

DS/ISP/INB will coordinate contracts requiring Sensitive Compartmented Information (SCI) access with the Bureau of Intelligence and Research (INR/EX/SB). *Personnel security clearances will be processed in accordance with the NISPOM Supplement.*

12 FAM 574 CONTRACTING RESPONSIBILITIES

12 FAM 574.1-1 Contracting Officer's Representatives (CORs)

(TL:DS-48; 9-28-95)

a. After consulting with applicable Department security elements, contracting officers' representatives (CORs) are responsible for identifying the security requirements which must be included in a contract (including personal/ professional services contracts). The COR must then assist DS/ISP/INB in preparing the Contractor Security Classification Specification, DD Form 254. DS/ISP/INB is ultimately responsible for approving the DD Form 254.

b. The COR is responsible for performing classification reviews during contract performance and upon contract completion, and must ensure compliance with all security requirements for the duration of the contract. The COR must notify DS/ISP/INB and the contracting officer of any changes in security requirements as they occur so that appropriate contract modifications may be issued.

c. An Industrial Security Functional Responsibilities chart is provided in 12 FAM 574 Exhibit 574.1 . This chart outlines primary responsibilities of the contracting officer, contracting officer's representative (COR) and DS/ISP/INB during the life of a contract.

12 FAM 574.2 Office of Information Security Technology, Information Security Programs Division, Industrial Security Branch

(TL:DS-48; 9-28-95)

DS/ISP/INB is responsible for the development, coordination, and implementation of plans, policies, standards, and procedures necessary to safeguard the Department's classified and sensitive unclassified information entrusted to the private sector, both within the U. S. and worldwide. These policies, standards, and procedures include, but are not limited to:

(1) Department of State contract processing;

(2) Contractor handling of Department of State classified/unclassified sensitive information;

(3) Contractor security clearance requirements;

(4) Department of State industrial security inspections.

NOTE: DS/ISP/INB serves as the liaison between the Department of State and the Defense Investigative Service concerning Department contractors who participate in the *National Industrial Security Program (NISP).* DS/ISP/INB serves as the final approving authority for all DD Form 254s issued by the Department, and provides general assistance to both the Department and contractors concerning security requirements. Instructions for preparing the DD Form 254 can be obtained from DS/ISP/INB.

12 FAM 574.3 Contracting Officers

(TL:DS-48; 9-28-95)

Contracting officers award classified and sensitive unclassified contracts and ensure that all appropriate contract documentation has been included in the contract package and subsequent contract modifications. Appropriate documentation includes the requisite DD Form 254 (for classified contracts) and contract security clauses. This responsibility extends to pre-contract, contract award, and post-contract actions. Sensitive unclassified contracts must include security clauses which provide for the protection of Department of State information and other assets, investigations of personnel in public trust positions, building pass requirements, etc.

NOTE: Contracting officers must be mindful of the processing times for facility and personnel clearances and provide sufficient time for the firms to obtain the required clearances.

12 FAM 574.4 Unit Security Officers

(TL:DS-48; 9-28-95)

Unit Security Officers are responsible for briefing contract or other private sector employees working in their assigned area(s) regarding applicable security requirements and procedures. DS/ISP/INB should be consulted if there are any security related problems/concerns with any contract/private sector employee.

12 FAM 574.5 Supervisors

(TL:DS-48; 9-28-95)

Department supervisors must give adequate guidance to contract/private sector employees concerning the specific security requirements unique to their assigned projects. Supervisors should ensure that:

(1) Contractor personnel fully understand the classified elements of their individual assignments and have security classification guidance for any classified information they receive or generate;

(2) Personnel attend required security briefings;

(3) Infractions/Violations are reported to the appropriate Unit Security Officer; and

(4) Any adverse information concerning contractor/private sector employees is reported to DS/ISP/INB.

12 FAM 574.6 Contract/Private Sector Employees

(TL:DS-48; 9-28-95)

Contract or private sector employees are responsible for complying with the Department's security regulations and procedures.

12 FAM 575 CONTRACT PROCESSING

12 FAM 575.1 Department Contracting Activities

(TL:DS-48; 9-28-95)

a. The Office of the Procurement Executive (A/OPE) delegates contracting authority for Department contracting activities. Only those persons A/OPE designates may negotiate, enter into, and award contracts to the private sector.

b. Department classified procurement actions (i.e. those which will require access to classified information) require a fully executed DD Form 254 to be included with each of the following:

(1) Invitation for bid;

(2) Request for proposal or quotation;

(3) Contract (a contract can be a letter contract, purchase order, or any other recognized contract vehicle); or

(4) Subcontract package.

NOTE: DD-254s are not applicable for personal/professional services contracts.

c. Unclassified contracts, which do not involve access to classified information, do not normally need to be reviewed by DS/ISP/INB. However, where security requirements may need to be formulated due to the sensitivity

of the project (e.g., physical protection requirements for Department of State information or other assets or background investigations on contractor personnel, etc.), DS/ISP/INB will coordinate these security requirements with the requesting office.

12 FAM 575.2 Other Contracting Activities

(TL:DS-56; 2-20-97)

The requirements outlined in 12 FAM 574 *are equally applicable* to contracts awarded by other contracting agencies on behalf of the Department of State (e.g., Small Business Administration, General Services Administration, etc.). It is imperative that DS/ISP/INB be advised when other contracting activities are awarding classified contracts for the Department. DS/ISP/INB is responsible for approving DD Forms 254 in these instances also.

12 FAM 575.3 Contract Clause(s)

(TL:DS-48; 9-28-95)

Contracting clauses governing security requirements are available through the Office of Procurement Executive (A/OPE) and should be included in all classified contracts.

12 FAM 575.4 Contract Performance

(TL:DS-48; 9-28-95)

The contracting officer, in consultation with the COR and DS/ISP/INB, is responsible for ensuring contractor compliance with all security requirements during contract performance. Changes in security requirements should be coordinated between the contracting officer, COR, and DS/ISP/INB.

12 FAM 575.5 Contract Completion

(TL:DS-48; 9-28-95)

The contracting officer is responsible for notifying DS/ISP/INB of the contract completion (final delivery of goods or services) or the termination of the contract. DS/ISP/INB will advise the contractor regarding the proper disposition of any classified material released to or generated by the contractor.

12 FAM 576 HANDLING CLASSIFIED INFORMATION

12 FAM 576.1 Releasing Classified Information to Contractors

(TL:DS-48; 9-28-95)

When, in performance of a classified contract or preparation of a bid or proposal, classified material must be transmitted/released to the contractor's physical location, DS/ISP/INB must verify the contractor's facility security clearance and storage capability prior to the release of classified information by any Department of State office. (See 12 FAM 573.1-1 .) Contact DS/ISP/INB for verification.

12 FAM 576.2 Need-to-Know Determination

(TL:DS-56; 2-20-97)

In addition to verifying the contractor's facility clearance, the possessor of classified information must determine that a contractor has a need-to-know for the information. The determination is based on the recipient's need, in the interest of national security, for access to, knowledge of, or possession of classified information to perform tasks or services essential to fulfilling a Department contract or program. Once this need-to-know is established, the classified mailing address can be obtained from DS/ISP/INB and the classified material transmitted to the contractor in accordance with 12 FAM 536 .

12 FAM 576.3 Verification Of Individual Personnel Clearances

(TL:DS-56; 2-20-97)

Prior to allowing individual contractor employees access to classified information while at Department of State sites, Department employees must ensure that the contractor employee has a valid personnel security clearance. The clearance must be at a level equal to or higher than the level of the classified information to which they will have access. When contractor personnel require access to classified information, verification can be made through the *Office of Investigations, Employee/Contractor Branch* (DSS/I/PSS/EC).

12 FAM 576.4 Reporting Requirements

(TL:DS-56; 2-20-97)

a. Immediately report all unauthorized disclosures of classified information to contractor personnel in writing to the Office of Information Security Technology, Information Security Programs Division, Program Applications Branch (DS/ISP/APB) by completing Optional Form 118 (Record of Violation). DS/ISP/APB will conduct an evaluation and investigation if warranted *and will advise DS/ISP/INB of the results.*

b. Department personnel as well as contractors shall immediately report any adverse information coming to their attention concerning any cleared contractor employees to DS/ISP/INB. (For the purpose of this requirement, cleared contractor employee includes employees of contracting firms, consultants, etc.; who are cleared under the Industrial Security Program.) Reports based on rumor or innuendo should not be made. The subsequent termination of employment of a contractor employee does not obviate the requirement to submit this report. The contracting firm shall submit a copy of their adverse information reports to DS/ISP/INB. In some cases, DS/ISP/INB may report the adverse information to DISCO directly.

12 FAM 576.5 Contractor Releases

(TL:DS-56; 2-20-97)

In accordance with *the National Industrial Security Program Operating Manual (NISPOM)* and the DD Form 254 for the contract, contractors shall clear with DS/ISP/INB all requests to release unclassified information pertaining to contracts containing national security information. This includes, but is not limited to:

(1) Requests for public releases of unclassified information pertaining to classified contracts;

(2) Requests by contractors for release of unclassified information at seminars, meetings, and symposia; and

(3) Unclassified sales literature, to include publication or distribution of brochures, promotional sales literature, or similar material containing classified information.

12 FAM 577 CLEARANCE PROCESSING

(TL:DS-56; 2-20-97)

a. Individuals will undergo one clearance process either by the Department of State, Bureau of Diplomatic Security (DS), or by DISCO. The position that the contractor will encumber determines which agency is to perform the investigation. Different forms are required for each type of processing. An explanation of requirements is outlined in 12 FAM 577.1 . In determining which agency will process the clearance request, use the following guidance.

b. DS/ICI/PSS must clear the following categories of contractor personnel:

(1) *FBO project directors;*

(2) Medical personnel;

(3) Contract interpreters/ translators/escorts;

(4) INM field personnel (pilots, advisors, etc.);

(5) Cleared American Personnel Program for Russia/Eastern European Posts;

(6) Work study interns;

(7) Private sector individuals who are not under contract but who require access to DOS Classified information;

(8) Contractor positions filled directly by the post (requests must be submitted through the appropriate geographic bureau);

(9) *Contractor positions with "staff-like-access," which is defined as an individual under contract who will occupy a position involved in the policy/decision-making process (such as a program manager or project director), or who occupies a sensitive position for which the Department requires a DS issued clearance. (DS/ISP/INB determines this on a case-by-case basis.)*

NOTE: These categories of individuals are not all inclusive.

c. DISCO will process clearances for all self-employed contractor positions not meeting the above criteria. Submit all clearance requests directly to DS/ICI/PSS.

12 FAM 577.1 Submitting Personnel Security Clearance Requests

(TL:DS-56; 2-20-97)

a. The contractor's employing office must submit all requests for personnel security clearances to *DS/ICI/PSS*. The requesting memo for a contractor clearance must include:

(1) Name of the individual to be processed, his or her work location and phone number;

(2) Level of clearance required;

(3) Contract number, with expiration date, under which the work is to be performed; and

(4) Area(s) to be accessed and a sufficient explanation of the proposed work, including work location and job title.

NOTE: The Department of State requires that its cleared contractors assigned overseas comply with DOS regulations (*3 FAM 4100, Appendix A*) requiring the investigation of intended foreign national spouses and cohabitants or certain established relationships with foreign nationals. Contractor employees will be counselled by DOS officials on the potential impact of such relationships on their continued acceptability for assignment overseas and will be provided the requisite forms for a DOS conducted investigation and evaluation.

b. The following forms are required for DS clearance processing:

(1) Questionnaire for Sensitive Positions, Standard Form 86. Individuals should submit an original and three copies. If the subject has a spouse, intended spouse, or cohabitant who is a foreign national, a Standard Form 86 (original and two copies) is required on the individual; it should be submitted with the subject's investigative package. If the spouse, intended spouse, or cohabitant is a naturalized citizen, also provide the following information:

(a) Naturalization certificate number;

(b) Date of naturalization; and

(c) City and state and court where naturalization occurred;

(2) Two completed fingerprint cards (Form FD-258). These cards must have the following code in the ORI block:

USDOS002Z, US DEPT OF STATE, WASH DC

(3) Statement as to how/where (phone number) the individual may be contacted.

NOTE: DS uses the Optional Form 184, Request for Biographic Data, to process clearance requests for attorneys representing employees, international conference participants, and textile advisors.

c. The contractor's employing office must submit a memorandum to DS/ICI/PSS to request an extension or revalidation of a DS issued clearance. *It is the employing office's responsibility to monitor the clearance status of personnel assigned to their area.* Include:

(1) Subject's name;

(2) Date of birth;

(3) Position title;

(4) Contract number and expiration date;

(5) Any change in level of clearance required; and

(6) Date of expiration.

d. For clearances which can be extended without further investigative processing (stamped at the bottom of the Department of State form, DS-1897 Certificate of Security Clearance for Access), only the memo is required. For clearances which cannot be extended without an update investigation (stamped at the bottom of the DS-1897), submit an SF-86 (original and three copies) and two FD-258s to DS/ICI/PSS in addition to the memo.

e. DISCO clearance forms which are available through DS/ICI/PSS include:

(1) *SF-86: Personnel Security Questionnaire which is used to process an individual for a clearance;*

(2) DD-1879: DoD Request for Personnel Security Investigation which must accompany the *SF-86;*

(3) Two completed fingerprint cards (Form FD-258). These cards must have the following code in the ORI block:

USDIS000Z, DIS NACC, FT HOLABIRD, MD

(4) Proof of citizenship. Provide a copy of the individual's birth certificate or passport. If the individual is a naturalized citizen, the requester must provide a statement that he or she has seen the official naturalization certificate, which may not be reproduced, and provide the certificate number,

date of naturalization, place (city and state) and court where naturalization occurred.

12 FAM 577.2 Visit Notification

(TL:DS-48; 9-28-95)

a. Firm employees who hold DISCO clearances and are assigned to or visiting Department of State facilities where access to classified information is required, must have their clearances certified by use of a visit authorization request (VAR). The firm shall submit all contractor visit authorization requests to DS/ISP/INB. DS/ISP/INB will verify the cited classified contract/ activity and, if approved, forward it to DS/ICI/PSS/EC for entry into the contractor clearance verification data base. Concurrent with this action, DS/ISP/INB will forward a copy of the visit request to the contracting officer's representative (COR) point-of-contact. That individual must certify that the cleared contractor(s) has/have a valid need-to-know for the contract/activity cited on the visit request. An interim Secret or Confidential PCL is valid for access to classified information at the level of the interim PCL granted, except for Sensitive Compartmented Information, Restricted Data, COMSEC Information, SAP, and NATO information. An interim Top Secret PCL is valid for access to Top Secret information and Restricted Data, NATO information and COMSEC information at the Secret and Confidential level. Unless otherwise notified by the contracting officer's representative (COR), DS/ISP/INB will consider the need-to-know certified and no further action will be taken by that office. If DS/ISP/INB does not approve the visit request, it will return the request to the company either requesting additional information or disapproving the proposed classified visit.

b. Department of State employees visiting contractor facilities where access to classified information is required or where classified discussions will occur must have their personnel security clearances certified by DSS/ICI/PSS/EC to the company being visited.

12 FAM 577.3 Contract Completion/Changes

(TL:DS-48; 9-28-95)

Report to DS/ISP/INB changes in a contractor's personnel security clearance status as follows:

(1) Firm employees: The firm is required to notify DS/ISP/INB when a cleared employee terminates, no longer requires access, or the personnel security clearance level changes;

(2) Self-employed individuals: The cognizant Department contracting organization must notify DS/ICI/PSS when the status of a cleared, self-employed contractor changes. Typical changes are employee termination,

transfer to another assignment within the Department requiring a higher or lower level of clearance or no longer requiring a clearance, etc.

12 FAM 578 INDUSTRIAL SECURITY EDUCATION PROGRAMS

12 FAM 578.1 General

(TL:DS-48; 9-28-95)

a. The effectiveness of the Department's industrial security program depends upon the understanding of private sector and U.S. Government participants of their respective security responsibilities. For this reason, education is an integral part of the Department's security program. The focus of the educational effort is to impress upon these individuals, through security briefings, their continuing responsibility to safeguard classified information.

b. Individuals must familiarize themselves with security regulations that relate to their assigned duties found in the *Foreign Affairs Manual*.

12 FAM 578.2 Required Briefings

12 FAM 578.2-1 Department of State Personnel

(TL:DS-48; 9-28-95)

DS/ISP/INB will brief Department personnel such as regional security officers (RSOs), contracting officer's representatives (CORs), program managers, site security managers, etc., on their responsibilities for proper implementation of the Department's Industrial Security Program. Areas to be covered include, but are not limited to, the following:

(1) Program overview;

(2) Classified contracts;

(3) Determination of contract classification;

(4) Facility clearance for prospective contractors;

(5) Preparation of security classification guidance;

(6) DD Form 254 (Contract Security Classification Specification);

(7) Visit request to Department of State facilities;

(8) Security classification reviews;

(9) Reciprocally cleared firms; and

(10) Foreign-owned, controlled, or influenced companies.

12 FAM 578.2-2 Contract Employees

(TL:DS-56; 2-20-97)

a. *DS/ISP/INB* will brief all personal/professional services contractors cleared for access to Department of State classified information or assigned duties requiring a trustworthiness determination with the Department of State on their security responsibilities. Areas covered include, but are not limited to, the following:

(1) Techniques employed by foreign intelligence services in attempting to obtain classified information and employee responsibility for reporting such attempts;

(2) Handling and protecting classified information;

(3) Prohibitions against disclosing classified information, by any means, to unauthorized persons; and

(4) Penalties that may be imposed for unauthorized disclosures and security infractions/violations.

b. The employee must sign a Classified Information Nondisclosure Agreement Standard Form 312 (SF-312) at the time of the security briefing. Access to classified information will not be authorized until this form has been executed. The RSO will brief personal/ professional services contractors located overseas.

c. When access to classified information is no longer required, DS/ISP/INB will debrief personal/professional services contractors. The RSO will debrief contractors separating overseas.

d. Firm employees under contract to the Department will be briefed by their Facility Security Officer in accordance with the *National Industrial Security Program (NISP).*

12 FAM 578.3 Counterintelligence Briefings

(TL:DS-48; 9-28-95)

The regional security officer assigned to a critical human intelligence threat post is responsible for administering a counterintelligence briefing upon the contractor's arrival at post and debriefing upon their departure. See 12 FAM 260 for further information regarding Counterintelligence Programs.

12 FAM 579 INSPECTION PROGRAM

12 FAM 579.1 Program Responsibility

(TL:DS-56; 2-20-97)

a. *It is the objective of the Department of State's Industrial Security Program to ensure that contractors who have entered into a contractual relationship with the Department involving access to classified information are abiding by the requirements outlined above.*

b. DS/ISP/INB is responsible for inspecting contractors performing on classified projects at Department of State locations domestically. RSOs and/or site security managers (SSMs) are responsible for inspecting contractors overseas. DS/CIS/PSP and *DS/DSS/OP* are responsible for follow-up actions during their overseas accreditation/inspection trips.

12 FAM 579.2 Scope

12 FAM 579.2-1 Domestic Inspections

(TL:DS-56; 2-20-97)

a. For contractors performing on classified projects at domestic DOS locations, DS/ISP/INB will conduct a pre-inspection survey by contacting the COR to determine the status of the contract, individuals assigned to the contract, any areas of concern.

b. Inspections focus on contractors' generation and protection of the Department's classified and/or unclassified sensitive information. DS/ISP/INB interviews contractor personnel to determine if employees have been properly briefed and understand their security responsibilities.

c. DS/ISP/INB provides a report of the inspection findings, with any corrective actions to be taken, to the contracting officer, COR and company facility security officer.

12 FAM 579.2-2 Overseas Inspections

(TL:DS-56; 2-20-97)

a. The following outlines the parameters of overseas inspections to be conducted by regional security officers and site security managers for contractors assigned to overseas Department of State facilities. Contractor employees refer to:

(1) Employees of firms possessing a facility security clearance; and

(2) Personal services contractor employees possessing appropriate security clearances.

b. The following outlines three areas of the Industrial Security Overseas Inspection Program: Pre-inspection research, the actual inspection and post-inspection guidance.

12 FAM 579.3 Pre-Inspection Research

(TL:DS-56; 2-20-97)

a. Prior to conducting an industrial security inspection at an overseas post, the RSO and/or SSM should complete a pre-inspection research checksheet for contractors assigned within that jurisdiction who are working on Department of State (DOS) classified contracts. Normally, RSOs are responsible for the inspection of any contractors working on Department of State contracts within the confines of existing DOS facilities, i.e., embassies and consulates. SSMs are responsible for DOS facilities under new construction, i.e., new office buildings (NOBs) and certain renovation projects. The following checksheet should be used by the RSO and/or the SSM as a basis for pre-inspection research prior to the actual inspection.

b. (Keep in mind that this checksheet is not all inclusive and, if deemed appropriate, can be expanded at the discretion of the RSO/SSM. The RSO/SSM should tailor this guide to individual situations at post.)

NOTE: Prior to the inspection, if available, a review of the contract, to include the Contract Security Classification Specification (DD Form 254), security classification guidance, Construction Security Specifications and Construction Security Plan should be accomplished.

12 FAM 579.3-1 Pre-Inspection Checklist

(TL:DS-56; 2-20-97)

A pre-inspection checklist includes:

(1) Names of contractor firms at post which require access to classified areas or classified information;

(2) Number of contractor employees at post;

(3) Who are the project managers at post for each contract?

(4) Are there cables on file indicating the clearance levels of all contractor employees?

(5) Where is classified information for contractor use stored?

(6) How do contractor employees access classified information (i.e., work with classified documents; have access to security combinations; review cable traffic; access classified areas)?

(7) Have the contractor employees been involved in any security incidents within the past year? Were they reported to DS/ISP/APB, if required?

12 FAM 579.3-2 Applicability

(TL:DS-56; 2-20-97)

a. Industrial security compliance inspections occur on an announced and unannounced basis at Department of State locations worldwide.

b. These inspections apply to contractor employees employed by a firm, as well as to personal/ professional services contractors.

12 FAM 579.3-3 Inspection Questionnaire

(TL:DS-56; 2-20-97)

To ensure that the overseas element of the Department's Industrial Security Program is adequately addressed, it is imperative that an inspection of contractor employees be conducted on an annual basis or at least once during a project (if the project is less than one year in duration). This inspection serves to ensure that contractors assigned overseas on classified contracts are adhering to the security requirements of their contract(s) with DOS. As such, the RSO/SSM should conduct interviews of contractor employees based upon the pre-inspection research information disclosed and the type of access the contractors are having at post. 12 FAM 579 Exhibit 579.3-3 *is a questionnaire provided for the RSO/SSM as a general guideline in conducting industrial security inspections of contractor employees. The interview questions should be utilized to elicit information*

from a representative sampling of contractor employees regarding their access to classified material and their adherence to security procedures.

12 FAM 579.3-4 Post-Inspection Guidance

(TL:DS-56; 2-20-97)

a. Based on the information obtained from both the pre-inspection research and inspection questionnaire, the RSO/SSM should provide an overall assessment of the contractor's adherence to DOS security requirements on-site. This assessment (in either cable or facsimile format) should be forwarded to: Chief, DS/ISP/INB; 2201 "C" Street, NW; Washington, D.C. 20520 (FAX Number 202-663-0686). (SSMs should forward the report through A/FBO/PE/CSM.) The following is provided for the RSO/SSM to use as a guide in determining their assessment of the contractors on site:

(1) Overall security posture: Excellent/Good/Fair/Poor;

(2) Are employees aware of their security responsibilities?

(3) Do the employees have a good understanding of the security requirements and do they follow through on them?

(4) Is there a pattern of security violations?

(5) Do contractors adhere to post reporting requirements?

b. After providing a brief narrative as to the overall assessment of the contractor's adherence to security requirements, also include any areas of concern or any possible follow-up actions required by DS/ISP/INB or other elements of the Department.

12 FAM 579.4 Industrial Security Violations Program

(TL:DS-56; 2-20-97)

The Defense Investigative Service (DIS) is responsible for monitoring contractor employees performing at contractor facilities and notifying DS/ISP/INB, if appropriate, of infractions/violations committed by the firm's employees performing on Department of State contracts. In the event of a compromise or suspected compromise, DS/ISP/APB will perform a classification review, coordinate a damage assessment, if necessary, and ensure that the Department takes appropriate action to mitigate any damage caused by the compromise. All such actions will be in coordination with the appropriate COR and contracting officer. Infractions/ violations by firm employees which occur at DOS locations will be adjudicated by

DS/ISP/APB, which in turn will provide a report of the infraction/violation to the firm and to DS/ISP/INB. DS/ISP/INB will notify DIS of the infraction/violation.

12 FAM 574 Exhibit 574.1
INDUSTRIAL SECURITY FUNCTIONAL RESPONSIBILITIES

FUNCTION	COR	DS/ISP/INB	CO	REMARKS
Determines contract security requirements	X	X		
Provides special contract security requirements (in addition to ISM); e.g., SAPs, SCI, TEMPEST, etc.	X	X		
Establishes security requirements by DD Form 254	X	X		
Reviews and signs DD Form 254		X		
Reviews contract for changes to security requirements	X	X		
Issues notice on review of classification		X		
Resolves classification problems		X		
Coordinates contractor requests for public release of information pertaining to classified contracts		X		
Coordinates requests and authorizes release of classified information by contractors at seminars, meetings, and symposia		X		
Initiates requests for facility security clearances		X		When requested by contracting officer
Coordinates requests and furnishes written authorization for publication and distribution of classified sales literature			X	
Advises contractor of method of shipment of classified material when required		X		
Authorizes classified visits		X		
Approves expenditure of funds for security requirements; e.g., area controls, storage equipment, protective alarm systems			X	
Ensures contractor compliance with all contract security requirements	X	X	X	
Reviews reports of security violations from DIS and determines appropriate action		X		
Approves use of secure electrical transmission systems				Accomplished by A/IM/SO/TO

FUNCTION	COR	DS/ISP/INB	CO	REMARKS
Approves need for COMSEC material for R&D, production, installation and maintenance				A/IM/SO/TO
Appoints contractor employees as COMSEC material couriers (after designated by contractor)				A/IM/SO/TO
Advises contractor of government represent–atives authorized access to controlled areas containing COMSEC material				A/IM/SO/TO
Furnishes written approval to contractors to permit prospective subcontractors, vendors, suppliers access to classified information		X		
Reviews contract deliverables to determine proper classification	X			DS/PSP/PSD for diplomatic construction contracts
Authorizes contractors to retain classified material upon contract completion or termination		X		

12 FAM 579 Exhibit 579.3-3
QUESTIONNAIRE FOR CONDUCTING INDUSTRIAL SECURITY INSPECTIONS OF CONTRACTOR EMPLOYEES

1. What is the employee's position with the contractor? How long has the employee been employed by the contractor? How long has the employee been at post?

2. Does the employee know what level of clearance he or she has (Secret or Top Secret)? Has the employee ever held a clearance before? If so, what level and with whom?

3. Was the employee briefed by his or her firm before arriving at post? What information was included in the security briefing? Does the employee recall signing a Non-Disclosure Agreement (SF-312)?

4. Does the employee have access to classified information? At what level; in what ways; how often? When was the last time the employee had access to classified information?

5. Does the employee have access to a classified computer system?

6. How does the employee handle classified material, i.e., storage, handling, and protection during duty and non-duty hours?

7. Do the contractor employees generate any classified material (i.e., reports, cables, plans)? If so, have they been provided with appropriate security classification guidance to generate classified material?

8. Does the employee have access to safe combinations? Where are these safe combinations stored? Are they written down anywhere?

9. Is the employee responsible for securing classified information at any time?

10. During the project, has the employee traveled to any critical threat posts that require security briefings? Were there any problems?

11. Is the employee aware of any security violations or does he or she have any concerns regarding security? Has the employee been involved in any security violations? If the employee was involved in any security violation(s), what was the outcome?