CHAPTER 1
General Provisions and Requirements

Section 1. Introduction

1-100. Purpose. This Manual is issued in accordance with the National Industrial Security Program (NISP). It prescribes the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information. The Manual controls the authorized disclosure of classified information released by U.S. Government Executive Branch Departments and Agencies to their contractors. It also prescribes the procedures, requirements, restrictions, and other safeguards to protect special classes of classified information, including Restricted Data (RD), Formerly Restricted Data (FRD), intelligence sources and methods information, Sensitive Compartmented Information (SCI), and Special Access Program (SAP) information. These procedures are applicable to licensees, grantees, and certificate holders to the extent legally and practically possible within the constraints of applicable law and the Code of Federal Regulations.

1-101. Authority

a. The NISP was established by Executive Order (E.O.) 12829 (reference (a)) for the protection of information classified under E.O. 12958 (reference (b)) as amended, or its successor or predecessor orders, and the Atomic Energy Act of 1954 (reference (c)), as amended. The National Security Council is responsible for providing overall policy direction for the NISP. The Secretary of Defense has been designated Executive Agent for the NISP by the President. 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. The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Chairman of the Nuclear Regulatory Commission (NRC) and the Director of the Central Intelligence Agency (CIA), is responsible for the issuance and maintenance of this Manual. The Secretary of Energy and the Chairman of the NRC are responsible for prescribing that portion of the Manual that pertains to information classified under reference (c), as amended. The Director of National Intelligence (DNI) is responsible for prescribing that portion of the Manual that pertains to intelligence sources and methods, including SCI. The DNI retains authority over access to intelligence sources and methods, including SCI. The Director of the CIA may inspect and monitor contractor, licensee, and grantee programs and facilities that involve access to such information. The Secretary of Energy and the Chairman of the NRC retain authority over access to information under their respective programs classified under reference (c) as amended. The Secretary or the Chairman may inspect and monitor contractor, licensee, grantee, and certificate holder programs and facilities that involve access to such information.

c. The Secretary of Defense serves as Executive Agent for inspecting and monitoring contractors, licensees, grantees, and certificate holders who require or will require access to, or who store or will store classified information; and for determining the eligibility for access to classified information of contractors, licensees, certificate holders, and grantees and their respective employees.

d. The Director, ISOO, will consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the NISP.

e. Nothing in this Manual shall be construed to supersede the authority of the Secretary of Energy or the Chairman of the NRC under reference (c). Nor shall this information detract from the authority of installation commanders under the Internal Security Act of 1950 (reference (d)); the authority of the Director of the Central Intelligence Agency under the National Security Act of 1947, as amended, (reference (e)) or E.O. 12333 (reference (f)); as amended by E.O. 13355 (reference (g)); or the authority of the DNI under the Intelligence Reform and Terrorism Prevention Act of 2004 (reference (h)). This Manual shall not detract from the authority of other applicable provisions of law, or the authority of any other Federal department or agency head granted according to U.S. statute or Presidential decree.

1-102. Scope

a. The NISP applies to all Executive Branch Departments and Agencies and to all cleared contractor facilities located within the United States and its territories.

b. This Manual applies to and shall be used by contractors to safeguard classified information released during all phases of the contracting, licensing, and grant process, including bidding, negotiation, award, performance, and termination. It also applies to classified information not released under a contract, license, certificate or grant, and to foreign government information furnished to contractors that requires protection in the interest of national security. This Manual implements applicable Federal Statutes, E.O.s, National Directives, international treaties, and certain government-to-government agreements.

c. Implementation of changes to this Manual by contractors shall be effected no later than 6 months from the date of the published change.

d. This Manual does not contain protection requirements for Special Nuclear Material.

1-103. Agency Agreements

a. Reference (a) requires the Heads of Agencies to enter into agreements with the Secretary of Defense as the Executive Agent for the NISP. This is designated by Presidential guidance that establishes the terms of the Secretary's responsibilities on behalf of these agency heads.

b. The Secretary of Defense has entered into agreements with the departments and agencies listed below for the purpose of rendering industrial security services. This delegation of authority is contained in an exchange of letters between the Secretary of Defense and (1) the Administrator, National Aeronautics and Space Administration (NASA); (2) the Secretary of Commerce; (3) the Administrator, General Services Administration (GSA); (4) the Secretary of State; (5) the Administrator, Small Business Administration (SBA); (6) the Director, National Science Foundation (NSF); (7) the Secretary of the Treasury; (8) the Secretary of Transportation; (9) the Secretary of the Interior; (10) the Secretary of Agriculture; (11) the Secretary of Labor; (12) the Administrator, Environmental Protection Agency (EPA); (13) the Attorney General, Department of Justice (DOJ); (14) the Chairman, Board of Governors, Federal Reserve System (FRS); (15) the Comptroller General of the United States, Government Accountability Office (GAO); (16) the Director of Administrative Services, United States Trade Representative (USTR); (17) the Director of Administration, United States International Trade Commission (USITC); (18) the Administrator, United States Agency for International Development (USAID); (19) the Executive Director for Operations of the NRC; (20) the Secretary of Education; (21) the Secretary of Health and Human Services; (22) the Secretary of Homeland Security; and (23) the Deputy Managing Director, Federal Communications Commission (FCC).

1-104. Security Cognizance

a. Consistent with paragraph 1-101e, security cognizance remains with each Federal department or agency unless lawfully delegated. The term Cognizant Security Agency (CSA) denotes the Department of Defense (DoD), the Department of Energy (DOE), the NRC, and the Central Intelligence Agency (CIA). The Secretary of Defense, the Secretary of Energy, the Director of the CIA and the Chairman, NRC, may delegate any aspect of security administration regarding classified activities and contracts under their purview within the CSA or to another CSA. Responsibility for security administration may be further delegated by a CSA to one or more Cognizant Security Offices (CSO). It is the obligation of each CSA to inform industry of the applicable CSO.

b. The designation of a CSO does not relieve any Government Contracting Activity (GCA) of the responsibility to protect and safeguard the classified information necessary for its classified contracts, or from visiting the contractor to review the security aspects of such contracts.

c. Nothing in this Manual affects the authority of the Head of an Agency to limit, deny, or revoke access to classified information under its statutory, regulatory, or contract jurisdiction if that Agency Head determines that the security of the nation so requires. The term "Agency Head" has the meaning provided in Title 5 United States Code (U.S.C.) Section 552(f) (reference (i)).

1-105. Composition of Manual. This Manual is comprised of a "baseline" portion (Chapters 1 through 11). The portion of the Manual that prescribes requirements, restrictions, and safeguards that exceed the baseline standards, such as those necessary to protect special classes of information, is included in the NISPOM Supplement

(NISPOMSUP). Until officially revised or canceled, the existing Carrier Supplement to the former "Industrial Security Manual for Safeguarding Classified Information" (reference (j)) will continue to be applicable to DoD-cleared facilities only.

1-106. Manual Interpretations. All contractor requests for interpretations of this Manual shall be forwarded to the CSA through its designated CSO. Requests for interpretation by contractors located on any U.S. Government installation shall be forwarded to the CSA through the commander or head of the host installation. Requests for interpretation of Director of Central Intelligence Directives (DCIDs) shall be forwarded to the DNI through approved channels.

1-107. Waivers and Exceptions to this Manual. Requests shall be submitted by industry through government channels approved by the CSA. When submitting a request for waiver, the contractor shall specify, in writing, the reasons why it is impractical or unreasonable to comply with the requirement. Waivers and exceptions will not be granted to impose more stringent protection requirements than this Manual provides for CONFIDENTIAL, SECRET, or TOP SECRET information.

Section 2. General Requirements

1-200. General. Contractors shall protect all classified information to which they have access or custody. A contractor performing work within the confines of a Federal installation shall safeguard classified information according to the procedures of the host installation or agency.

1-201. Facility Security Officer (FSO). The contractor shall appoint a U.S. citizen employee, who is cleared as part of the facility clearance (FCL) to be the FSO. The FSO will supervise and direct security measures necessary for implementing applicable requirements of this Manual and related Federal requirements for classified information. The FSO, or those otherwise performing security duties, shall complete security training as specified in Chapter 3 and as deemed appropriate by the CSA.

1-202. Standard Practice Procedures. The contractor shall implement all applicable terms of this Manual at each of its cleared facilities. Written procedures shall be prepared when the FSO believes them to be necessary for effective implementation of this Manual or when the CSA determines them to be necessary to reasonably exclude the possibility of loss or compromise of classified information.

1-203. One-Person Facilities. A facility at which only one person is assigned shall establish procedures for CSA notification after death or incapacitation of that person. The current combination of the facility's security container shall be provided to the CSA, or in the case of a multiple facility organization, to the home office.

1-204. Cooperation with Federal Agencies and Officially Credentialed Representatives of Those Agencies. Contractors shall cooperate with Federal agencies and their officially credentialed representatives during official inspections, investigations concerning the protection of classified information, and during personnel security investigations of present or former employees and others. Cooperation includes providing suitable arrangements within the facility for conducting private interviews with employees during normal working hours, providing relevant employment and security records for review when requested, and rendering other necessary assistance.

1-205. Security Training and Briefings. Contractors are responsible for advising all cleared employees, including those outside the United States, of their individual responsibility for safeguarding classified information. In this regard, contractors shall provide security training as appropriate, according to Chapter 3, to cleared employees by initial briefings, refresher briefings, and debriefings.

1-206. Security Reviews

a. **Government Reviews.** Aperiodic security reviews of all cleared contractor facilities will be conducted to ensure that safeguards employed by contractors are adequate for the protection of classified information.

(1) **Review Cycle.** The CSA will determine the frequency of security reviews, which may be increased or decreased consistent with risk management principles. Security reviews may be conducted not more often than once every 12 months unless special circumstances exist.

(2) **Procedures.** Contractors will normally be provided notice of a forthcoming review. Unannounced reviews may be conducted at the discretion of the CSA. Security reviews necessarily subject all contractor employees and all areas and receptacles under the control of the contractor to examination. However, every effort will be made to avoid unnecessary intrusion into the personal effects of contractor personnel. The physical examination of the interior space of equipment not authorized to secure classified material will always be accomplished in the presence of a representative of the contractor.

(3) **Reciprocity.** Each CSA is responsible for ensuring that redundant and duplicative security review and audit activity of its contractors is held to a minimum, including such activity conducted at common facilities by other CSA's. Appropriate intra- and/or inter-agency agreements shall be executed to avoid redundant and duplicate reviews. Instances of redundant and duplicative security review and audit activity shall be reported to the Director, ISOO, for resolution.

b. **Contractor Reviews.** Contractors shall review their security system on a continuing basis and shall also conduct a formal self-inspection at intervals consistent with risk management principles.

1-207. Hotlines. Federal agencies maintain hotlines to provide an unconstrained avenue for government

and contractor employees to report, without fear of reprisal, known or suspected instances of serious security irregularities and infractions concerning contracts, programs, or projects. These hotlines do not supplant contractor responsibility to facilitate reporting and timely investigation of security matters concerning its operations or personnel, and contractor personnel are encouraged to furnish information through established company channels. However, the hotline may be used as an alternate means to report this type of information when considered prudent or necessary. Contractors shall inform all employees that the hotlines may be used, if necessary, for reporting matters of national security significance. CSA hotline addresses and telephone numbers are as follows:

Defense Hotline
The Pentagon
Washington, DC 20301-1900
(800) 424-9098

NRC Hotline
U.S. Nuclear Regulatory Commission
Office of the Inspector General
Mail Stop TSD 28
Washington, D.C. 20555-0001
(800) 233-3497

CIA Hotline
Office of the Inspector General
Central Intelligence Agency
Washington, D.C. 20505
(703) 874-2600

DOE Hotline
Department of Energy
Office of the Inspector General
1000 Independence Avenue, S.W. Room 5A235
Washington, D.C. 20585
(202) 586-4073
(800) 541-1625

1-208. Classified Information Procedures Act (CIPA) (Public Law. 96-456, 94 Stat. 2025 codified at Title 18 U.S.C. Appendix 3 (reference (k))). The CIPA provides procedures for access to classified information by defendants and their representatives in criminal proceedings in U.S. District Courts, Courts of Appeal, and the U.S. Supreme Court. The provisions of this Manual do not apply to criminal proceedings in the courts and do not authorize contractors or their employees to release classified information in connection with any criminal proceedings.

Section 3. Reporting Requirements

1-300. General. Contractors are required to report certain events that have an impact on the status of the facility clearance (FCL), that impact on the status of an employee's personnel security clearance (PCL), that affect proper safeguarding of classified information, or that indicate classified information has been lost or compromised. Contractors shall establish such internal procedures as are necessary to ensure that cleared employees are aware of their responsibilities for reporting pertinent information to the FSO, the Federal Bureau of Investigation (FBI), or other Federal authorities as required by this Manual, the terms of a classified contract, and U.S. law. Contractors shall provide complete information to enable the CSA to ascertain whether classified information is adequately protected. Contractors shall submit reports to the FBI and to their CSA as specified in this section.

a. When the reports are classified or offered in confidence and so marked by the contractor, the information will be reviewed by the CSA to determine whether it may be withheld from public disclosure under applicable exemptions of the Freedom of Information Act (5 U.S.C. 552) (reference (l)).

b. When the reports are unclassified and contain information pertaining to an individual, the Privacy Act of 1974 (5 U.S.C. 552a)(reference (m)) permits withholding of that information from the individual only to the extent that the disclosure of the information would reveal the identity of a source who furnished the information to the U.S. Government under an expressed promise that the identity of the source would be held in confidence. The fact that a report is submitted in confidence must be clearly marked on the report.

1-301 Reports to be Submitted to the FBI. The contractor shall promptly submit a written report to the nearest field office of the FBI regarding information coming to the contractor's attention concerning actual, probable or possible espionage, sabotage, terrorism, or subversive activities at any of its locations. An initial report may be made by phone, but it must be followed in writing, regardless of the disposition made of the report by the FBI. A copy of the written report shall be provided to the CSA.

1-302 Reports to be Submitted to the CSA

a. Adverse Information. Contractors shall report adverse information coming to their attention concerning any of their cleared employees. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. If the individual is employed on a Federal installation, the contractor shall furnish a copy of the report and its final disposition to the commander or head of the installation.

NOTE: In two court cases, Becker vs. Philco and Taglia vs. Philco (389 U.S. 979), the U.S. Court of Appeals for the 4th Circuit decided on February 6, 1967, that a contractor is not liable for defamation of an employee because of reports made to the Government under the requirements of this Manual and its previous versions.

b. Suspicious Contacts. Contractors shall report efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information or to compromise a cleared employee. In addition, all contacts by cleared employees with known or suspected intelligence officers from any country, or any contact which suggests the employee concerned may be the target of an attempted exploitation by the intelligence services of another country shall be reported.

c. Change in Cleared Employee Status. Contractors shall report: (1) the death; (2) a change in name; (3) the termination of employment; (4) change in citizenship; and (5) when the possibility of access to classified information in the future has been reasonably foreclosed. The CSA shall designate the appropriate reporting mechanism.

d. Citizenship by Naturalization. Contractors shall report if a non-U.S. citizen employee granted a Limited Access Authorization (LAA) becomes a citizen through naturalization. The report shall include: (1) city, county, and state where naturalized; (2) date naturalized; (3) court; and (4) certificate number.

e. Employees Desiring Not to Perform on Classified Work. Contractors shall report that an employee no longer wishes to be processed for a clearance or to continue an existing clearance.

f. Standard Form (SF) 312. Refusal by an employee to execute the "Classified Information Nondisclosure Agreement" (SF 312).

g. Change Conditions Affecting the Facility Clearance

(1) Any change of ownership, including stock transfers that affect control of the company.

(2) Any change of operating name or address of the company or any of its cleared locations.

(3) Any change to the information previously submitted for key management personnel including, as appropriate, the names of the individuals they are replacing. In addition, a statement shall be made indicating (a) whether the new key management personnel are cleared, and if so, to what level and when, their dates and places of birth, social security numbers, and their citizenship; (b) whether they have been excluded from access; or (c) whether they have been temporarily excluded from access pending the granting of their clearance. A new complete listing of key management personnel need be submitted only at the discretion of the contractor and/or when requested by the CSA.

(4) Action to terminate business or operations for any reason, imminent adjudication or reorganization in bankruptcy, or any change that might affect the validity of the FCL.

(5) Any material change concerning the information previously reported by the contractor concerning foreign ownership, control or influence (FOCI). This report shall be made by the submission of a Certificate Pertaining to Foreign Interests. When submitting this information, it is not necessary to repeat answers that have not changed. When entering into discussions, consultations or agreements that may reasonably lead to effective ownership or control by a foreign interest, the contractor shall report the details by letter. If the contractor has received a Schedule 13D from the investor, a copy shall be forwarded with the report.

h. Changes in Storage Capability. Any change in the storage capability that would raise or lower the level of classified information the facility is approved to safeguard.

i. Inability to Safeguard Classified Material. Any emergency situation that renders the facility incapable of safeguarding classified material.

j. Security Equipment Vulnerabilities. Significant vulnerabilities identified in security equipment, intrusion detection systems (IDS), access control systems, communications security (COMSEC) equipment or systems, and information system (IS) security hardware and software used to protect classified material.

k. Unauthorized Receipt of Classified Material. The receipt or discovery of any classified material that the contractor is not authorized to have. The report should identify the source of the material, originator, quantity, subject or title, date, and classification level.

l. Employee Information in Compromise Cases. When requested by the CSA, information concerning an employee when the information is needed in connection with the loss, compromise, or suspected compromise of classified information.

m. Disposition of Classified Material Terminated From Accountability. When the whereabouts or disposition of classified material previously terminated from accountability is subsequently determined.

n. Foreign Classified Contracts. Any precontract negotiation or award not placed through a GCA that involves, or may involve: (1) the release or disclosure of U.S. classified information to a foreign interest or (2) access to classified information furnished by a foreign interest.

1-303. Reports of Loss, Compromise, or Suspected Compromise. Any loss, compromise or suspected compromise of classified information, foreign or domestic, shall be reported to the CSA. Classified material that cannot be located within a reasonable period of time shall be presumed to be lost until an investigation determines otherwise. If the facility is located on a Government installation, the report shall be furnished to the CSA through the Commander or Head of the host installation.

a. Preliminary Inquiry. Immediately on receipt of a report of loss, compromise, or suspected compromise of classified information, the contractor shall initiate a preliminary inquiry to ascertain all of the circumstances surrounding the reported loss, compromise or suspected compromise.

b. Initial Report. If the contractor's preliminary inquiry confirms that a loss, compromise, or suspected compromise of any classified

information occurred, the contractor shall promptly submit an initial report of the incident unless otherwise notified by the CSA. Submission of the initial report shall not be deferred.

c. Final Report. When the investigation has been completed, a final report shall be submitted to the CSA. The report should include:

(1) Material and relevant information that was not included in the initial report;

(2) The name and social security number of the individual(s) who was primarily responsible for the incident, including a record of prior loss, compromise, or suspected compromise for which the individual had been determined responsible;

(3) A statement of the corrective action taken to preclude a recurrence and the disciplinary action taken against the responsible individual(s), if any; and

(4) Specific reasons for reaching the conclusion that loss, compromise, or suspected compromise occurred or did not occur.

1-304. Individual Culpability Reports. Contractors shall establish and enforce policies that provide for appropriate administrative actions taken against employees who violate requirements of this Manual. They shall establish and apply a graduated scale of disciplinary actions in the event of employee violations or negligence. A statement of the administrative actions taken against an employee shall be included in a report to the CSA when individual responsibility for a security violation can be determined and one or more of the following factors are evident:

a. The violation involved a deliberate disregard of security requirements.

b. The violation involved gross negligence in the handling of classified material.

c. The violation involved was not deliberate in nature but involves a pattern of negligence or carelessness.

CHAPTER 2
Security Clearances

Section 1. Facility Clearances (FCLs)

2-100. General. An FCL is an administrative determination that a company is eligible for access to classified information or award of a classified contract. Contract award may be made prior to the issuance of an FCL. In those cases, the contractor will be processed for an FCL at the appropriate level and must meet eligibility requirements for access to classified information. However, the contractor will not be afforded access to classified information until the FCL has been granted. The FCL requirement for a prime contractor includes those instances in which all classified access will be limited to subcontractors. Contractors are eligible for custody (possession) of classified material if they have an FCL and storage capability approved by the CSA.

a. An FCL is valid for access to classified information at the same or lower classification level as the FCL granted.

b. FCLs will be registered centrally by the U.S. Government.

c. A contractor shall not use its FCL for advertising or promotional purposes.

2-101. Reciprocity. An FCL shall be considered valid and acceptable for use on a fully reciprocal basis by all Federal departments and agencies, provided it meets or exceeds the level of clearance needed.

2-102. Eligibility Requirements. A contractor or prospective contractor cannot apply for its own FCL. A GCA or a currently cleared contractor may sponsor an uncleared company for an FCL. A company must meet the following eligibility requirements before it can be processed for an FCL:

a. The company must need access to the classified information in connection with a legitimate U.S. Government or foreign government requirement.

b. The company must be organized and existing under the laws of any of the fifty states, the District of Columbia, or Puerto Rico, and be located in the United States or its territorial areas.

c. The company must have a reputation for integrity and lawful conduct in its business dealings. The company and its key managers must not be barred from participating in U.S. Government contracts.

d. The company must not be under FOCI to such a degree that the granting of the FCL would be inconsistent with the national interest.

2-103. Processing the FCL. The CSA will advise and assist the company during the FCL process. As a minimum, the company will:

a. Execute CSA-designated forms.

b. Process key management personnel for PCLs.

c. Appoint a U.S. citizen employee as the FSO.

2-104. PCLs Required in Connection with the FCL. The senior management official and the FSO must always be cleared to the level of the FCL. Other officials, as determined by the CSA, must be granted PCLs or be excluded from classified access pursuant to paragraph 2-106.

2-105. PCLs Concurrent with the FCL. Contractors may designate employees who require access to classified information during the negotiation of a contract or the preparation of a bid or quotation pertaining to a prime contract or a subcontract to be processed for PCLs concurrent with the FCL. The granting of an FCL is not dependent on the clearance of such employees.

2-106. Exclusion Procedures. When, pursuant to paragraph 2-104, formal exclusion action is required, the organization's board of directors or similar executive body shall affirm the following, as appropriate.

a. 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 disclosed to the organization. They also do not occupy positions that would enable them to adversely affect the organization's policies or practices in the

performance of classified contracts. This action shall be made a matter of record by the organization's executive body. A copy of the resolution shall be furnished to the CSA.

b. Such officers or partners (designated by name) shall not require, shall not have, and can be effectively denied access to higher-level classified information (specify which higher level(s)) and do not occupy positions that would enable them to adversely affect the organization's policies or practices in the performance of higher-level classified contracts (specify higher level(s)). This action shall be made a matter of record by the organization's executive body. A copy of the resolution shall be furnished to the CSA.

2-107. Interim FCLs. An interim FCL may be granted to eligible contractors by the CSA. An interim FCL is granted on a temporary basis pending completion of the full investigative requirements.

2-108. Multiple Facility Organizations (MFOs). The home office facility must have an FCL at the same, or higher, level of any cleared facility within the MFO. The CSA shall determine the necessity for branch offices to be cleared.

2-109. Parent-Subsidiary Relationships. When a parent-subsidiary relationship exists, the parent and the subsidiary will be processed separately for an FCL. As a general rule, the parent must have an FCL at the same, or higher, level as the subsidiary. However, the CSA will determine the necessity for the parent to be cleared or excluded from access to classified information. The CSA will advise the companies as to what action is necessary for processing the FCL. When a parent or its cleared subsidiaries are collocated, a formal written agreement to use common security services may be executed by the two firms, subject to the approval of the CSA.

2-110. Termination of the FCL. Once granted, an FCL remains in effect until terminated by either party. If the FCL is terminated for any reason, the contractor shall return all classified material in its possession to the appropriate GCA or dispose of the material as instructed by the CSA.

2-111. Records Maintenance. Contractors shall maintain the original CSA designated forms for the duration of the FCL.

Section 2. Personnel Security Clearances

2-200. General

a. An employee may be processed for a PCL when the contractor determines that access is essential in the performance of tasks or services related to the fulfillment of a classified contract. A PCL is valid for access to classified information at the same or lower level of classification as the level of the clearance granted.

b. The CSA will determine eligibility for access to classified information in accordance with the national standards and notify the contractor that eligibility has been granted. The CSA will notify the contractor when an employee's PCL has been denied, suspended, or revoked. The contractor shall immediately deny access to classified information to any employee when notified of a denial, revocation or suspension. When the CSA has designated a database as the system of record for contractor eligibility and access, the contractor shall be responsible for annotating and maintaining the accuracy of their employees' access records. Specific procedures will be provided by the CSA.

c. Within an MFO or within the same corporate family, contractors may centrally manage eligibility and access records.

d. The contractor shall limit requests for PCLs to the minimal number of employees necessary for operational efficiency, consistent with contractual obligations and other requirements of this Manual. Requests for PCLs shall not be made to establish "pools" of cleared employees.

e. The contractor shall not submit a request for a PCL to one agency if the employee applicant is cleared or is in process for a PCL by another agency. In such cases, to permit clearance verification, the contractor should provide the new agency with the full name, date and place of birth, social security number, clearing agency and type of investigation

f. Access to SCI and SAP information is a determination made by the granting authority.

2-201. Investigative Requirements. Investigations conducted by a Federal agency shall not be duplicated by another Federal agency when those investigations are current within 5 years and meet the scope and standards for the level of PCL required. The types of investigations required are as follows:

a. Single Scope Background Investigation (SSBI). An SSBI is required for TOP SECRET, Q, and SCI access. Investigative requests shall be made using the electronic version of the Questionnaire for National Security Positions (SF 86).

b. National Agency Check with Local Agency Check and Credit Check (NACLC). An NACLC is required for a SECRET, L, and CONFIDENTIAL PCLs. Investigative requests shall be made using the electronic version of the SF 86.

c. Polygraph. Agencies with policies sanctioning the use of the polygraph for PCL purposes may require polygraph examinations when necessary. If issues of concern surface during any phase of security processing, coverage will be expanded to resolve those issues.

d. Reinvestigation. Contractor personnel may be subject to a reinvestigation program as specified by the CSA.

e. Financial Disclosure. When advised by the GCA that an employee is required to complete a Financial Disclosure Form, the contractor shall ensure that the employee has the opportunity to complete and submit the form in private.

2-202. Procedures for Completing the Electronic Version of the SF 86. The electronic version of the SF 86 shall be completed jointly by the employee and the FSO or an equivalent contractor employee(s) who has (have) been specifically designated by the contractor to review an employee's SF 86.

a. The FSO or designee shall inform the employee that the SF 86 is subject to review and shall review the application solely to determine its adequacy and to ensure that necessary information has not been omitted. The FSO or designee shall provide the employee with written notification that review of the information is for adequacy and completeness, information will be used for no other purpose within the company, and that the information provided by the employee is protected by reference (m). The FSO or designee shall not share information from the employee's SF 86 within the company and shall not use the information for any

purpose other than determining the adequacy and completeness of the SF 86.

b. The FSO or designee shall ensure that the applicant's fingerprints are authentic, legible, and complete to avoid subsequent clearance processing delays. The FSO or designee shall retain an original, signed copy of the SF 86, the Authorization for Release of Information and Records, and Authorization for Release of Medical Information until the clearance process has been completed. The FSO or designee shall maintain the retained documentation in such a manner that the confidentiality of the documents is preserved and protected against access by anyone within the company other than the FSO or designee. When the applicant's eligibility for access to classified information has been granted or denied, the retained documentation shall be destroyed.

2-203. Common Adjudicative Standards. Security clearance and SCI access determinations are based upon uniform common adjudicative standards.

2-204. Reciprocity. Federal agencies that grant access to classified information to their employees or their contractor employees are responsible for determining whether such employees have been previously cleared or investigated by the Federal Government. Any previously granted PCL that is based upon a current investigation of a scope that meets or exceeds that necessary for the clearance required shall provide the basis for issuance of a new clearance without further investigation or adjudication unless significant derogatory information that was not previously adjudicated becomes known to the granting agency.

2-205. Pre-employment Clearance Action. If access to classified information is required by a potential employee immediately upon commencement of their employment, a PCL application may be submitted to the CSA by the contractor prior to the date of employment provided a written commitment for employment has been made by the contractor, and the candidate has accepted the offer in writing. The commitment for employment will indicate that employment shall commence within 30 days of the granting of eligibility for a PCL.

2-206. Contractor-Granted Clearances. Contractors are no longer permitted to grant clearances. Contractor-granted CONFIDENTIAL clearances in effect under previous policy are not valid for access to RD, FRD, COMSEC information, SCI, NATO information (except RESTRICTED), and classified foreign government information (FGI), or for Critical or Controlled Nuclear Weapon Security positions.

2-207. Verification of U.S. Citizenship. The contractor shall require each applicant for a PCL who claims U.S. citizenship to produce evidence of citizenship.

2-208. Acceptable Proof of Citizenship

a. For individuals born in the United States, a birth certificate is the primary and preferred means of citizenship verification. Acceptable certificates must show that the birth record was filed shortly after birth and it must be certified with the registrar's signature. It must bear the raised, impressed, or multicolored seal of the registrar's office. The only exception is if a State or other jurisdiction does not issue such seals as a matter of policy. Uncertified copies of birth certificates are not acceptable. A delayed birth certificate is one created when a record was filed more than one year after the date of birth. Such a certificate is acceptable if it shows that the report of birth was supported by acceptable secondary evidence of birth. Secondary evidence may include: baptismal or circumcision certificates, hospital birth records, or affidavits of persons having personal knowledge about the facts of birth. Other documentary evidence can be early census, school, or family bible records, newspaper files, or insurance papers. All documents submitted as evidence of birth in the U.S. shall be original or certified documents.

b. If the individual claims citizenship by naturalization, a certificate of naturalization is acceptable proof of citizenship.

c. If citizenship was acquired by birth abroad to a U.S. citizen parent or parents, the following are acceptable evidence:

(1) A Certificate of Citizenship issued by the Department of Homeland Security, U.S. Citizenship and Immigration Services (USCIS) or its predecessor organization.

(2) A Report of Birth Abroad of a Citizen of the United States of America

(3) A Certificate of Birth.

d. A passport, current or expired, is acceptable proof of citizenship.

e. A Record of Military Processing-Armed Forces of the United States (DD Form 1966) is acceptable proof of citizenship, provided it reflects U.S. citizenship.

2-209. Non-U.S. Citizens. Only U.S. citizens are eligible for a security clearance. Every effort shall be made to ensure that non-U.S. citizens are not employed in duties that may require access to classified information. However, compelling reasons may exist to grant access to classified information to a non-U.S. citizen. Such individuals may be granted a Limited Access Authorization (LAA) in those rare circumstances where the non-U.S. citizen possesses unique or unusual skill or expertise that is urgently needed to support a specific U.S. Government contract involving access to specified classified information and a cleared or clearable U.S. citizen is not readily available. In addition, the LAA may be processed only with the concurrence of the GCA.

2-210. Access Limitations of an LAA. An LAA granted under the provisions of this Manual is not valid for access to the following types of information:

a. TOP SECRET information.

b. RD or FRD.

c. Information that has not been determined releasable by a U.S. Government designated disclosure authority to the country of which the individual is a citizen.

d. COMSEC information.

e. Intelligence information.

f. NATO Information. However, foreign nationals of a NATO member nation may be authorized access to NATO Information provided that: (1) A NATO Security Clearance Certificate is obtained by the CSA from the individual's home country; and (2) NATO access is limited to performance on a specific NATO contract.

g. Information for which foreign disclosure has been prohibited in whole or in part; and

h. Information provided to the U.S. Government in confidence by a third party government and classified information furnished by a third party government.

2-211. Interim PCLs. Applicants for TOP SECRET, SECRET, and CONFIDENTIAL PCLs may be routinely granted interim PCLs, as appropriate, provided there is no evidence of adverse information of material significance. The interim status will cease if results are favorable following completion of full investigative requirements. Non-U.S. citizens are not eligible for access to classified information on an interim basis.

a. An interim SECRET or CONFIDENTIAL PCL is valid for access to classified information at the level of the eligibility granted, except for RD, COMSEC Information, and NATO information. An interim TOP SECRET PCL is valid for access to TOP SECRET information, RD, NATO Information, and COMSEC information at the SECRET and CONFIDENTIAL level. Access to SCI and SAP information based on an interim PCL is a determination made by the granting authority.

b. An interim PCL granted by the CSA negates any existing contractor-granted CONFIDENTIAL clearance. When an interim PCL has been granted and derogatory information is subsequently developed, the CSA may withdraw the interim pending completion of the processing that is a prerequisite to the granting of a final PCL.

c. When an interim PCL for an individual who is required to be cleared in connection with the FCL is withdrawn, the individual must be removed from access or the interim FCL will also be withdrawn.

d. Withdrawal of an interim PCL is not a denial or revocation of the clearance and may not be appealed.

2-212. Consultants. A consultant is an individual under contract to provide professional or technical assistance to a contractor in a capacity requiring access to classified information. The consultant shall not possess classified material off the premises of the using (hiring) contractor except in connection with authorized visits. The consultant and the using contractor shall jointly execute a consultant certificate setting forth respective security responsibilities. The using contractor shall be the consumer of the services offered by the consultant it sponsors for a PCL. For security administration purposes, the consultant shall be considered an employee of the using contractor. Consultants to GCAs shall be processed for PCLs by the GCA in accordance with GCA procedures.

Section 3. Foreign Ownership, Control, or Influence (FOCI)

2-300. Policy. Foreign investment can play an important role in maintaining the vitality of the U.S. industrial base. Therefore, it is the policy of the U.S. Government to allow foreign investment consistent with the national security interests of the United States. The following FOCI policy for U.S. companies subject to an FCL is intended to facilitate foreign investment by ensuring that foreign firms cannot undermine U.S. security and export controls to gain unauthorized access to critical technology, classified information, and special classes of classified information.

a. A U.S. company is considered under FOCI whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

b. Whenever a company has been determined to be under FOCI, the primary consideration shall be the safeguarding of classified information. The CSA is responsible for taking whatever interim action is necessary to safeguard classified information, in coordination with other affected agencies as appropriate.

c. A U.S. company determined to be under FOCI is ineligible for an FCL unless and until security measures have been put in place to negate or mitigate FOCI. When a contractor determined to be under FOCI is negotiating an acceptable FOCI mitigation/negation measure, an existing FCL shall continue so long as there is no indication that classified information is at risk of compromise. An existing FCL shall be invalidated if the contractor is unable or unwilling to negotiate an acceptable FOCI mitigation/negation measure. An existing FCL shall be revoked if security measures cannot be taken to remove the possibility of unauthorized access or adverse affect on classified contracts.

d. If the company does not have possession of classified material, and does not have a current or impending requirement for access to classified information, the FCL shall be administratively terminated.

e. Changed conditions, such as a change in ownership, indebtedness, or the foreign intelligence threat, may justify certain adjustments to the security terms under which a company is operating or, alternatively, that a different FOCI negation method be employed. If a changed condition is of sufficient significance, it might also result in a determination that a company is no longer considered to be under FOCI or, conversely, that a company is no longer eligible for an FCL.

f. The Federal Government reserves the right and has the obligation to impose any security method, safeguard, or restriction it believes necessary to ensure that unauthorized access to classified information is effectively precluded and that performance of classified contracts is not adversely affected.

g. Nothing contained in this section shall affect the authority of the Head of an Agency to limit, deny or revoke access to classified information under its statutory, regulatory or contract jurisdiction. For purposes of this section, the term "Agency" has the meaning provided at reference (i), to include the term "DoD Component."

2-301. Factors. The following factors relating to the company, the foreign interest, and the government of the foreign interest, as appropriate, shall be considered in the aggregate to determine whether an applicant company is under FOCI, its eligibility for an FCL, and the protective measures required:

a. Record of economic and government espionage against U.S. targets.

b. Record of enforcement and/or engagement in unauthorized technology transfer.

c. The type and sensitivity of the information that shall be accessed.

d. The source, nature and extent of FOCI, including whether foreign interests hold a majority or substantial minority position in the company, taking into consideration the immediate, intermediate, and ultimate parent companies. A minority position is deemed substantial if it consists of greater than 5 percent of the ownership interests or greater than 10 percent of the voting interest.

e. Record of compliance with pertinent U.S. laws, regulations and contracts.

f. The nature of any bilateral and multilateral security and information exchange agreements that may pertain.

g. Ownership or control, in whole or in part, by a foreign government.

2-302. Procedures. A company is required to complete a Certificate Pertaining to Foreign Interests when applying for an FCL or when significant changes occur to information previously submitted. In the case of a corporate family, the form shall be a consolidated response rather than separate submissions from individual members of the corporate family.

a. If there are any affirmative answers on the Certificate Pertaining to Foreign Interests, or other information is received which indicates that the applicant company may be under FOCI, the CSA shall review the case to determine the relative significance of the information in regard to:

(1) Whether the applicant is under FOCI,

(2) The extent and manner to which the FOCI may result in unauthorized access to classified information or adversely impact classified contract performance; and

(3) The type of actions, if any, that would be necessary to negate the effects of FOCI to a level deemed acceptable to the Federal Government. Disputed matters may be appealed and the applicant shall be advised of the government's appeal channels by the CSA.

b. When a contractor with an FCL enters into negotiations for the proposed merger, acquisition, or takeover by a foreign interest, the contractor shall submit notification to the CSA of the commencement of such negotiations. The submission shall include the type of transaction under negotiation (stock purchase, asset purchase, etc.), the identity of the potential foreign interest investor, and a plan to negate the FOCI by a method outlined in 2-303. The company shall submit copies of loan, purchase and shareholder agreements, annual reports, bylaws, articles of incorporation, partnership agreements, and reports filed with other Federal agencies to the CSA.

c. When factors not related to ownership are present, positive measures shall assure that the foreign interest can be effectively mitigated and cannot otherwise adversely affect performance on classified contracts. Examples of such measures include modification or termination of loan agreements, contracts and other understandings with foreign interests; diversification or reduction of foreign-source income; demonstration of financial viability independent of foreign interests; elimination or resolution of problem debt; assignment of specific oversight duties and responsibilities to board members; formulation of special executive-level security committees to consider and oversee matters that affect the performance of classified contracts; physical or organizational separation of the contractor component performing on classified contracts; the appointment of a technology control officer; adoption of special Board Resolutions; and other actions that negate or mitigate foreign influence.

2-303. FOCI Action Plans. The following are the methods that can be applied to negate or mitigate the risk of foreign ownership or control.

a. Board Resolution. When a foreign interest does not own voting interests sufficient to elect, or otherwise is not entitled to representation on the company's governing board, a resolution(s) by the governing board shall normally be adequate. The governing board shall identify the foreign shareholder and describe the type and number of foreign-owned shares; acknowledge the company's obligation to comply with all industrial security program and export control requirements; and certify that the foreign owner does not require, shall not have, and can be effectively precluded from unauthorized access to all classified and export-controlled information entrusted to or held by the company. The governing board shall provide for annual certifications to the CSA acknowledging the continued effectiveness of the resolution. The company shall distribute to members of its governing board and to its key management personnel copies of such resolutions, and report in the company's corporate records the completion of such distribution.

b. Voting Trust Agreement and Proxy Agreement. The Voting Trust Agreement and the Proxy Agreement are arrangements whereby the foreign owner relinquishes most rights associated with ownership of the company to cleared U.S. citizens approved by the U.S. Government. Under a Voting Trust Agreement, the foreign owner transfers legal title in the company to the Trustees. Under a

Proxy Agreement, the foreign owner's voting rights are conveyed to the Proxy Holders. Neither arrangement imposes any restrictions on the company's eligibility to have access to classified information or to compete for classified contracts.

(1) Establishment of a Voting Trust or Proxy Agreement involves the selection of Trustees or Proxy Holders, all of whom must become members of the company's governing board. Both arrangements must provide for the exercise of all prerogatives of ownership by the Trustees or Proxy Holders with complete freedom to act independently from the foreign owners, except as provided in the Voting Trust or Proxy Agreement. The arrangements may, however, limit the authority of the Trustees or Proxy Holders by requiring that approval be obtained from the foreign owner(s) with respect to matters such as:

(a) The sale or disposal of the company's assets or a substantial part thereof;

(b) Pledges, mortgages, or other encumbrances on the company's assets, capital stock or ownership interests;

(c) Mergers, consolidations, or reorganizations;

(d) Dissolution; and

(e) Filing of a bankruptcy petition.

However, the Trustees or Proxy Holders may consult with the foreign owner, or vice versa, where otherwise consistent with U.S. laws, regulations and the terms of the Voting Trust or Proxy Agreement.

(2) The Trustees or Proxy Holders assume full responsibility for the foreign owner's voting interests and for exercising all management prerogatives relating thereto in such a way as to ensure that the foreign owner shall be insulated from the company, thereby solely retaining the status of a beneficiary. The company must be organized, structured, and financed so as to be capable of operating as a viable business entity independent from the foreign owner.

c. **Special Security Agreement (SSA) and Security Control Agreement (SCA).** The SSA and SCA are arrangements that, based upon an assessment of the FOCI factors, impose various industrial security and export control measures within an institutionalized set of company practices and procedures. They require active involvement in security matters of senior management and certain Board members (outside directors), who must be cleared U.S. citizens; provide for the establishment of a Government Security Committee (GSC) to oversee classified and export control matters; and preserve the foreign owner's right to be represented on the Board (inside directors) with a direct voice in the business management of the company while denying unauthorized access to classified information.

(1) When a company is not effectively owned or controlled by a foreign interest and the foreign interest is nevertheless entitled to representation on the company's governing board, the company may be cleared under an SCA. There are no access limitations under an SCA.

(2) A company that is effectively owned or controlled by a foreign interest may be cleared under an SSA arrangement. Access to proscribed information[1] by a company cleared under an SSA may require that the GCA complete a National Interest Determination (NID) to determine that release of proscribed information to the company shall not harm the national security interests of the United States. The CSA shall advise the GCA on the need for a NID.

(a) The NID can be program, project or contract specific. A separate NID is not required for each contract under a program or project. The NID decision shall be made at the GCA's Program Executive Office level. If the proscribed information is under the classification or control jurisdiction of another agency, the GCA shall advise that agency; e.g., National Security Agency (NSA) for COMSEC, DNI for SCI, DOE for RD. These agencies may determine that release to the contractor of an entire category of information under their control may not harm the national security.

(b) The GCA shall forward the completed NID to the CSA. The CSA shall not delay implementation of a FOCI action plan pending completion of a GCA's NID process as long as there is no indication that a NID shall be denied.

2-304. Citizenship of Persons Requiring PCLs. Under all methods of FOCI mitigation or negation, management positions requiring PCLs in conjunction

[1] Proscribed information includes TS, COMSEC except classified keys used for data transfer, RD as defined in reference (c), SAP, and SCI.

with the FCL must be filled by U.S. citizens residing in the United States.

2-305. Qualifications of Trustees, Proxy Holders, and Outside Directors. Individuals who serve as Trustees, Proxy Holders, or Outside Directors must be:

a. Resident U.S. citizens who can exercise management prerogatives relating to their position in a way that ensures that the foreign owner can be effectively insulated from the company;

b. Except as approved by the CSA in advance and in writing, completely disinterested individuals with no prior involvement with the company, the entities with which it is affiliated, or the foreign owner; and

c. Issued a PCL at the level of the facility's FCL.

2-306. GSC. Under a Voting Trust, Proxy Agreement, SSA and SCA, the contractor is required to establish a permanent committee of its Board of Directors, known as the GSC.

a. Unless otherwise approved by the CSA, the GSC consists of Voting Trustees, Proxy Holders or Outside Directors, as applicable, and those officers/directors who hold PCLs.

b. The members of the GSC are required to ensure that the contractor maintains policies and procedures to safeguard classified and export controlled information entrusted to it, and that violations of those policies and procedures are promptly investigated and reported to the appropriate authority when it has been determined that a violation has occurred.

c. The GSC shall also take the necessary steps to ensure that the contractor complies with U.S. export control laws and regulations and does not take action deemed adverse to performance on classified contracts. This shall include the appointment of a Technology Control Officer (TCO) and the establishment of Technology Control Plan (TCP).

d. The contractor's FSO shall be the principal advisor to the GSC and attend GSC meetings. The Chairman of the GSC must concur with the appointment and replacement of FSOs selected by management. The FSO and TCO functions shall be carried out under the authority of the GSC.

2-307. TCP. A TCP approved by the CSA shall be developed and implemented by those companies cleared under a Voting Trust Agreement, Proxy Agreement, SSA and SCA and when otherwise deemed appropriate by the CSA. The TCP shall prescribe all security measures determined necessary to reasonably foreclose the possibility of inadvertent access by non-U.S. citizen employees and visitors to information for which they are not authorized. The TCP shall also prescribe measures designed to assure that access by non-U.S. citizens is strictly limited to only that specific information for which appropriate Federal Government disclosure authorization has been obtained; e.g., an approved export license or technical assistance agreement. Unique badging, escort, segregated work area, security indoctrination schemes, and other measures shall be included, as appropriate.

2-308. Annual Review and Certification

a. Annual Review. The CSA shall meet at least annually with the GSCs of contractors operating under a Voting Trust, Proxy Agreement, SSA, or SCA to review the purpose and effectiveness of the clearance arrangement and to establish common understanding of the operating requirements and their implementation. These reviews shall also include an examination of the following:

(1) Acts of compliance or noncompliance with the approved security arrangement, standard rules, and applicable laws and regulations;

(2) Problems or impediments associated with the practical application or utility of the security arrangement; and

(3) Whether security controls, practices, or procedures warrant adjustment.

b. Annual Certification. For contractors operating under a Voting Trust Agreement, Proxy Agreement, SSA or SCA, the Chairman of the GSC shall submit to the CSA one year from the effective date of the agreement and annually thereafter an implementation and compliance report. Such reports shall include the following:

(1) A detailed description of the manner in which the contractor is carrying out its obligations under the agreement;

(2) Changes to security procedures, implemented or proposed, and the reasons for those changes;

(3) A detailed description of any acts of noncompliance, whether inadvertent or intentional, with a discussion of steps that were taken to prevent such acts from recurring;

(4) Any changes, or impending changes, of key management personnel or key board members, including the reasons therefore;

(5) Any changes or impending changes in the organizational structure or ownership, including any acquisitions, mergers or divestitures; and

(6) Any other issues that could have a bearing on the effectiveness of the applicable agreement.

2-309. Limited FCL. The United States has entered into Industrial Security Agreements with certain foreign governments. Some of these agreements establish arrangements whereby a foreign-owned U.S. company may be considered eligible for an FCL without any additional FOCI negation or mitigation instrument. Access limitations are inherent with the granting of Limited FCLs and are imposed upon all of the company's employees regardless of citizenship.

a. A Limited FCL may be granted upon satisfaction of the following criteria:

(1) There is an Industrial Security Agreement with the foreign government of the country from which the foreign ownership is derived.

(2) Release of classified information is in conformity with the U.S. National Disclosure Policy. Key management personnel may be citizens of the country of ownership for whom the United States has obtained security assurances at the appropriate level.

b. In extraordinary circumstances, a Limited FCL may also be granted even if the above criteria cannot be satisfied if there is a compelling need to do so consistent with U.S. national security interests. In any such case, the GCA shall provide a compelling need statement to the CSA to justify the FCL and verify that access to classified information is essential for contract performance. The CSA shall acknowledge the existence of a Limited FCL only to that GCA.

2-310. Foreign Mergers, Acquisitions and Takeovers, and the Committee on Foreign Investment in the United States (CFIUS)

a. The CFIUS, an interagency committee chaired by the Treasury Department, conducts reviews of proposed mergers, acquisition or takeovers of U.S. persons by foreign interests under section 721 (Exon-Florio amendment) of the Defense Production Act (reference (n)). CFIUS review is a voluntary process and affords an opportunity to foreign persons and U.S. persons entering into a covered transaction to submit the transaction for review by CFIUS to assess the impact of the transaction on U.S. national security.

b. The CFIUS review and the CSA industrial security FOCI review are carried out in two parallel but separate processes with different time constraints and considerations.

c. If a transaction under CFIUS review would require FOCI negation or mitigation measures if consummated, the CSA shall promptly advise the parties to the transaction and request that they submit to the CSA a plan to negate or mitigate FOCI. If it appears that an agreement cannot be reached on material terms of a FOCI action plan, or if the U.S. party to the proposed transaction fails to comply with the FOCI reporting requirements of this Manual, the CSA may recommend a full investigation of the transaction by CFIUS to determine the effects on national security.

d. If the CSA becomes aware of a proposed transaction that should be reviewed by CFIUS, and the parties thereto do not file a joint voluntary notice with CFIUS to initiate review within a reasonable time, the CSA shall initiate action to have CFIUS notified.

CHAPTER 3
Security Training and Briefings

Section 1. Security Training and Briefings

3-100. General. Contractors shall provide all cleared employees with security training and briefings commensurate with their involvement with classified information.

3-101. Training Materials. Contractors may obtain defensive security, threat awareness, and other education and training information and material from their CSA or other sources.

3-102. FSO Training. Contractors shall be responsible for ensuring that the FSO, and others performing security duties, complete security training considered appropriate by the CSA. Training requirements shall be based on the facility's involvement with classified information and may include an FSO orientation course and for FSOs at facilities with safeguarding capability, an FSO Program Management Course. Training, if required, should be completed within 1 year of appointment to the position of FSO.

3-103. Government-Provided Briefings. The CSA is responsible for providing initial security briefings to the FSO and for ensuring that other briefings required for special categories of information are provided.

3-104. Temporary Help Suppliers. A temporary help supplier, or other contractor who employs cleared individuals solely for dispatch elsewhere, shall be responsible for ensuring that required briefings are provided to their cleared personnel. The temporary help supplier or the using contractor may conduct these briefings.

3-105. Classified Information Nondisclosure Agreement (SF 312). The SF 312 is an agreement between the United States and an individual who is cleared for access to classified information. An employee issued an initial PCL must execute an SF 312 prior to being granted access to classified information. The contractor shall forward the executed SF 312 to the CSA for retention. If the employee refuses to execute the SF 312, the contractor shall deny the employee access to classified information and submit a report to the CSA. The SF 312 shall be signed and dated by the employee and witnessed. The employee's and witness' signatures must bear the same date.

3-106. Initial Security Briefings. Prior to being granted access to classified information, an employee shall receive an initial security briefing that includes the following:

a. A threat awareness briefing.

b. A defensive security briefing.

c. An overview of the security classification system.

d. Employee reporting obligations and requirements.

e. Security procedures and duties applicable to the employee's job.

3-107. Refresher Training. The contractor shall provide all cleared employees with some form of security education and training at least annually. Refresher training shall reinforce the information provided during the initial security briefing and shall keep cleared employees informed of appropriate changes in security regulations. Training methods may include group briefings, interactive videos, dissemination of instructional materials, or other media and methods. Contractors shall maintain records about the programs offered and employee participation in them. This requirement may be satisfied by use of distribution lists, facility/department-wide newsletters, or other means acceptable to the FSO.

3-108. Debriefings. Contractors shall debrief cleared employees at the time of termination of employment (discharge, resignation, or retirement); when an employee's PCL is terminated, suspended, or revoked; and upon termination of the FCL.

CHAPTER 4
Classification and Marking

Section 1. Classification

4-100. General. Information is classified under reference (b) by an original classification authority and is designated and marked as TOP SECRET, SECRET, or CONFIDENTIAL. The designation UNCLASSIFIED is used to identify information that does not require a security classification. Except as provided by statute, no other terms may be used to identify classified information.

4-101. Original Classification. An original classification decision at any level can be made only by a U.S. Government official who has been delegated the authority in writing. A determination to originally classify information may be made only when (a) an original classification authority is classifying the information; (b) the information falls into one or more of the categories set forth in reference (b); (c) the unauthorized disclosure of the information, either by itself or in context with other information, reasonably could be expected to cause damage to the national security, which includes defense against transnational terrorism, that can be identified or described by the original classifier; and (d) the information is owned by, produced by or for, or is under the control of the U. S. Government. The original classifier must state the concise "Reason" for classification on the front of the document. The original classifier must also indicate either a date or event for the duration of classification for up to 10 years from the date of the original classification decision unless the date is further extended due to information sensitivities for up to 25 years.

4-102. Derivative Classification Responsibilities

a. Contractors who extract or summarize classified information, or who apply classification markings derived from a source document, or are directed by a classification guide or a Contract Security Classification Specification, are making derivative classification decisions. The FSO shall ensure that all employees authorized to perform derivative classification actions are sufficiently trained and that they possess, or have ready access to, the pertinent classification guides and/or guidance necessary to fulfill these important actions. Any specialized training required to implement these responsibilities will be provided by the CSA upon request.

b. Employees who copy or extract classified information from another document, or who reproduce or translate an entire document, shall be responsible:

(1) For marking the new document or copy with the same classification markings as applied to the information or document from which the new document or copy was prepared and

(2) For challenging the classification if there is reason to believe the information is classified unnecessarily or improperly.

c. For information derivatively classified based on multiple sources, the derivative classifier shall: (1) carry forward the date or event for declassification that corresponds to the longest period of classification among the sources, and (2) maintain a listing of those sources on or attached to the official file or record copy.

d. Commensurate with their involvement, all personnel who have access to classified information shall be provided with security classification guidance.

4-103. Security Classification Guidance. The GCA is responsible for incorporating appropriate security requirements clauses in a classified contract, Invitation for Bid (IFB), Request for Proposal (RFP), Request for Quotation (RFQ), or other solicitation, and for providing the contractor with the security classification guidance needed during the performance of the contract. This guidance is provided to the contractor by the Contract Security Classification Specification. The Contract Security Classification Specification must identify the specific elements of classified information involved in the contract that require security protection.

a. Contractors shall, to the extent practicable, advise and assist in the development of the original Contract Security Classification Specification. It is the contractor's responsibility to understand and apply all aspects of the classification guidance. Users of classification guides are also encouraged to notify the originator of the guide when they acquire

information that suggests the need for change in the instructions contained in the guide. Classification guidance is, notwithstanding the contractor's input, the exclusive responsibility of the GCA, and the final determination of the appropriate classification for the information rests with that activity. The Contract Security Classification Specification is a contractual specification necessary for performance on a classified contract. If a classified contract is received without a Contract Security Classification Specification, the contractor shall advise the GCA.

b. The GCA is required to review the existing guidance periodically during the performance stages of the contract and to issue a revised Contract Security Classification Specification when a change occurs to the existing guidance or when additional security classification guidance is needed by the contractor.

c. Upon completion of a classified contract, the contractor must dispose of the classified information according to Chapter 5, Section 7. If the GCA does not advise to the contrary, the contractor may retain classified material for a period of 2 years following completion of the contract. The Contract Security Classification Specification will continue in effect for this 2-year period. If the GCA determines the contractor has a continuing need for the material, the GCA must issue a final Contract Security Classification Specification for the classified contract. A final specification is provided to show the retention period and to provide final disposition instructions for the classified material under the contract.

4-104. Challenges to Classification. Should a contractor believe (a) that information is classified improperly or unnecessarily; or (b) that current security considerations justify downgrading to a lower classification or upgrading to a higher classification; or (c) that the security classification guidance is improper or inadequate, the contractor shall discuss such issues with the pertinent GCA for remedy. If a solution is not forthcoming, and the contractor believes that corrective action is still required, a formal written challenge shall be made to the GCA. Such challenges shall include a description sufficient to identify the issue, the reasons why the contractor believes that corrective action is required, and any recommendations for appropriate corrective action. In any case, the information in question shall be safeguarded as required by this Manual for its assigned or proposed level of classification, whichever is higher, until action is completed. If no written answer is received within 60 days, the CSA should be requested to provide assistance in obtaining a response. If no response is received from the GCA within 120 days, the contractor may also forward the challenge to the Interagency Security Classification Appeals Panel (ISCAP) through the ISOO. The fact that a contractor has initiated such a challenge will not, in any way, serve as a basis for adverse action by the Government. If a contractor believes that adverse action did result from a classification challenge, full details should be furnished promptly to the ISOO for resolution.

4-105. Contractor Developed Information. Whenever a contractor develops an unsolicited proposal or originates information not in the performance of a classified contract, the following rules shall apply:

a. If the information was previously identified as classified, it shall be classified according to an appropriate Contract Security Classification Specification, classification guide, or source document, and marked as required by this Chapter.

b. If the information was not previously classified, but the contractor believes the information may or should be classified, the contractor should protect the information as though classified at the appropriate level and submit it to the agency that has an interest in the subject matter for a classification determination. In such a case, the following marking, or one that clearly conveys the same meaning, may be used:

CLASSIFICATION DETERMINATION PENDING
Protect as though classified (TOP SECRET,
SECRET, or CONFIDENTIAL).

This marking shall appear conspicuously at least once on the material but no further markings are necessary until a classification determination is received. In addition, contractors are not precluded from marking such material as company-private or proprietary information. Pending a final classification determination, the contractor should protect the information. It should be noted however, that reference (b) prohibits classification of information over which the Government has no jurisdiction. To be eligible for classification, the information must: (1) incorporate classified information to which the contractor was given prior access, or (2) the Government must first acquire a proprietary interest in the information.

4-106. Classified Information Appearing in Public Media. The fact that classified information has been

made public does not mean that it is automatically declassified. Contractors shall continue the classification until formally advised to the contrary. Questions about the propriety of continued classification in these cases should be brought to the immediate attention of the GCA.

4-107. Downgrading or Declassifying Classified Information. Information is downgraded or declassified based on the loss of sensitivity of the information due to the passage of time or on occurrence of a specific event. Contractors downgrade or declassify information based on the guidance provided in a Contract Security Classification Specification or upon formal notification. If material is marked for automatic declassification, the contractor shall seek guidance from the GCA prior to taking any action. Downgrading or declassifying actions constitute implementation of a directed action rather than an exercise of the authority for deciding the change or cancellation of the classification. At the time the material is actually downgraded or declassified, the action to update records and change the classification markings shall be initiated and performed. Declassification is not automatically an approval for public disclosure.

Section 2. Marking Requirements

4-200. General. Physically marking classified information with appropriate classification markings serves to warn and inform holders of the information of the degree of protection required. Other notations facilitate downgrading, declassification, and aid in derivative classification actions. Therefore, it is essential that all classified information and material be marked to clearly convey to the holder the level of classification assigned, the portions that contain or reveal classified information, the period of time protection is required, and any other notations required for protection of the information.

4-201. Marking Requirements for Information and Material. As a general rule, the markings specified in paragraphs 4-202 through 4-208 are required for all classified information regardless of the form in which it appears. Some material, such as documents, letters, and reports, can be easily marked with the required markings. Marking other material, such as equipment, IS media, and slides may be more difficult due to size or other physical characteristics. Since the primary purpose of the markings is to alert the holder that the information requires special protection, it is essential that all classified material be marked to the fullest extent possible to ensure the necessary safeguarding.

4-202. Identification Markings. All classified material shall be marked to show the name and address of the contractor responsible for its preparation, and the date of preparation. These markings are required on the face of all classified documents.

4-203. Overall Markings. The highest level of classified information contained in a document is its overall marking. The overall marking shall be conspicuously marked or stamped at the top and bottom on the outside of the front cover, on the title page, on the first page, and on the outside of the back. All copies of classified documents shall also bear the required markings. Overall markings shall be stamped, printed, etched, written, engraved, painted, or affixed by means of a tag, sticker, decal, or similar device on classified material other than documents, and on containers of such material, if possible. If marking the material or container is not practical, written notification of the markings shall be furnished to recipients.

4-204. Page Markings. Interior pages of classified documents shall be conspicuously marked or stamped at the top and bottom with the highest classification of the information appearing thereon, or the designation UNCLASSIFIED, if all the information on the particular page is UNCLASSIFIED. Alternatively, the overall classification of the document may be conspicuously marked or stamped at the top and bottom of each interior page, when necessary to achieve production efficiency, and the particular information to which classification is assigned is adequately identified by portion markings according to paragraph 4-206.

4-205. Component Markings. The major components of complex documents are likely to be used separately. In such cases, each major component shall be marked as a separate document. Examples include: (a) each annex, appendix, or similar component of a plan, program, or project description; (b) attachments and appendices to a letter; and (c) each major part of a report. If an entire major component is UNCLASSIFIED, the first page of the component may be marked at the top and bottom with the designation UNCLASSIFIED and a statement included, such as: "All portions of this (annex, appendix, etc.) are UNCLASSIFIED." When this method of marking is used, no further markings are required on the unclassified major component.

4-206. Portion Markings. Each section, part, paragraph, or similar portion of a classified document shall be marked to show the highest level of its classification, or that the portion is unclassified. Portions of documents shall be marked in a manner that eliminates doubt as to which of its portions contain or reveal classified information. Classification levels of portions of a document shall be shown by the appropriate classification symbol placed immediately following the portion's letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion. In marking portions, the parenthetical symbols (TS) for TOP SECRET, (S) for SECRET, (C) for CONFIDENTIAL, and (U) for UNCLASSIFIED shall be used.

a. Illustrations, photographs, figures, graphs, drawings, charts, or similar portions contained in classified documents shall be marked clearly to show their classified or unclassified status. These classification markings shall not be abbreviated and

shall be prominent and placed within or contiguous to such a portion. Captions of such portions shall be marked on the basis of their content.

b. If, in an exceptional situation, marking of the portions is determined to be impractical, the classified document shall contain a description sufficient to identify the exact information that is classified and the classification level(s) assigned to it. For example, each portion of a document need not be separately marked if all portions are classified at the same level, provided a full explanation is included in the document.

4-207. Subject and Title Markings. Unclassified subjects and titles shall be selected for classified documents, if possible. A classified subject or title shall be marked with the appropriate symbol placed immediately following the item.

4-208. Markings for Derivatively Classified Documents. All classified information shall be marked to reflect the source of the classification and declassification instructions. Documents shall show the required information either on the cover, first page, title page, or in another prominent position. Other material shall show the required information on the material itself or, if not practical, in related or accompanying documentation.

a. "DERIVED FROM" Line. The purpose of the "Derived From" line is to link the derivative classification applied to the material by the contractor and the source document(s) or classification guide(s) under which it was classified. In completing the "Derived From" line, the contractor shall identify the applicable guidance that authorizes the classification of the material. Normally this will be a security classification guide listed on the Contract Security Classification Specification or a source document. When identifying a classification guide on the "Derived From" line, the guide's title or number, issuing agency, and date shall be included. Many Contract Security Classification Specifications cite more than one classification guide and/or the contractor is extracting information from more than one classified source document. In these cases, the contractor may use the phrase "multiple sources." When the phrase "multiple sources" is used, the contractor shall maintain records that support the classification for the duration of the contract under which the material was created. These records may take the form of a bibliography identifying the applicable classification sources and be included in the text of the document or they may be maintained with the file or record copy of the document. When practical, this information should be included in or with all copies of the derivatively classified document. If the only source for the derivative classification instructions is the Contract Security Classification Specification, the date of the specification and the specific contract number for which it was issued shall be included on the "Derived From" line.

b. "DECLASSIFY ON" Line. The purpose of the "Declassify On" line is to provide declassification instructions appropriate for the material. When completing this line, the contractor shall use the information specified in the Contract Security Classification Specification or classification guide furnished with a classified contract. Or, the contractor shall carry forward the duration instruction from the source document or classification guide (e.g., date or event). When the source is marked "Original Agency's Determination Required" (OADR) or "X1 through X8", the "Declassify On" line should indicate that the source material was marked with one of these instructions and the date of origin of the most recent source document as appropriate to the circumstances. When a document is classified derivatively on the basis of more than one source document or more than one element of a classification guide, the "Declassify On" line shall reflect the longest duration of any of its sources. Material containing RD or FRD shall not have a "Declassify On" line.

c. "DOWNGRADE TO" Line. When downgrading instructions are contained in the Contract Security Classification Specification, classification guide or source document a "Downgrade To" line will be included. When completing this line, the contractor shall insert SECRET or CONFIDENTIAL and an effective date or event. The markings used to show this information are:

DERIVED FROM

DOWNGRADE TO ON

DECLASSIFY ON

d. "CLASSIFIED BY" Line and "REASON CLASSIFIED" Line. As a general rule, a "Classified By" line and a "Reason Classified" line will be shown only on originally classified documents. However, certain agencies may require that derivatively classified documents contain a "Classified By" line to identify the derivative classifier and a "Reason Classified" Line to identify

the specific reason for the derivative classification. Instructions for the use of these lines will be included in the security classification guidance provided with the contract.

4-209. Documents Generated Under Previous E.O.s. Documents classified under previous E.O.s need not be re-marked to comply with the marking requirements of reference (b).

a. Classified material originated under recent E.O.s contains overall, portion, paragraph, and appropriate downgrading and declassification markings that will provide sufficient guidance for the classification of extracted information. However, classified material originated under previous E.O.s may not have these markings. If the source document does not contain portion markings, the overall classification of the source document shall be used for the extracted information in the new document.

b. The classification markings for a source document are the responsibility of the originator and not the contractor extracting the information. Contractors are encouraged to contact the originator to avoid improper or unnecessary classification of material.

4-210. Marking Special Types of Material. The following procedures are for marking special types of material, but are not all inclusive. The intent of the markings is to ensure that the classification of the item, regardless of its form, is clear to the holder.

a. Files, Folders, or Groups of Documents. Files, folders, binders, envelopes, and other items containing classified documents, when not in secure storage, shall be conspicuously marked with the highest classification of any classified item included in the group. Cover sheets may be used for this purpose.

b. E-mail and other Electronic Messages. Electronically transmitted messages shall be marked in the same manner required for other documents except as noted. The overall classification of the message shall be the first item of information in the text. A "Derived From" line is required on messages. Certain agencies may also require that messages contain a "Classified By" and a "Reason Classified" line in order to identify the derivative classifier and the specific reason for classification. Instructions for the use of such lines will be included in the security classification guidance provided with the contract documents. When messages are printed by an automated system, all markings may be applied by that system, provided the classification markings are clearly distinguished from the printed text. The last line of text of the message shall include the declassification instructions.

c. Microforms. Microforms contain images or text in sizes too small to be read by the unaided eye. The applicable markings shall be conspicuously marked on the microform medium or its container to be readable by the unaided eye. These markings shall also be included on the image so that when the image is enlarged and displayed or printed, the markings will be conspicuous and readable. Further markings and handling shall be as appropriate for the particular microform involved.

d. Translations. Translations of U.S. classified information into a language other than English shall be marked to show the United States as the country of origin, with the appropriate U.S. markings and the foreign language equivalent.

4-211. Marking Transmittal Documents. A transmittal document shall be marked with the highest level of classified information contained in the document and with an appropriate notation to indicate its classification when the enclosures are removed. An unclassified document that transmits a classified document as an attachment shall bear a notation substantially as follows: "Unclassified when Separated from Classified Enclosures." A classified transmittal that transmits higher classified information shall be marked with a notation substantially as follows: "CONFIDENTIAL (or SECRET) when Separated from Enclosures." In addition, a classified transmittal itself must bear all the classification markings required for a classified document.

4-212. Marking Wholly Unclassified Material. Normally, wholly UNCLASSIFIED material will not be marked or stamped UNCLASSIFIED unless it is essential to convey to a recipient of such material that (a) the material has been examined specifically with a view to impose a security classification and has been determined not to require classification; or (b) the material has been reviewed and has been determined to no longer require classification and it is declassified.

4-213. Marking Compilations. In some instances, certain information that would otherwise be unclassified when standing alone may require classification when combined or associated with other unclassified information. When classification

is required to protect a compilation of such information, the overall classification assigned to the compilation shall be conspicuously affixed. The reason for classifying the compilation shall be stated at an appropriate location at or near the beginning of the compilation. In this instance, the portions of a compilation classified in this manner need not be marked.

4-214. Marking Miscellaneous Material. Material developed in connection with the handling, processing, production, and utilization of classified information shall be handled in a manner that ensures adequate protection of the classified information involved and shall be destroyed at the earliest practical time, unless a requirement exists to retain such material. There is no requirement to mark such material.

4-215. Marking Training Material. Unclassified documents or material that are created to simulate or demonstrate classified documents or material shall be clearly marked to indicate the actual UNCLASSIFIED status of the information. For example: SECRET FOR TRAINING PURPOSES ONLY, OTHERWISE UNCLASSIFIED or UNCLASSIFIED SAMPLE, or a similar marking may be used.

4-216. Downgrading or Declassification Actions. When documents or material that have been downgraded or declassified are removed from storage for use or for transmittal outside the facility, they shall be re-marked according to paragraph a or b below. If the volume of material is such that prompt re-marking of each classified item cannot be accomplished without unduly interfering with operations, a downgrading and declassification notice may be attached to the inside of the file drawers or other storage container instead of the re-marking otherwise required. Each notice shall specify the authority for the downgrading or declassification action, the date of the action, and the storage container to which it applies. When documents or other material subject to downgrading or declassification are withdrawn from the container solely for transfer to another, or when the container is transferred from one place to another, the transfer may be made without re-marking if the notice is attached to the new container or remains with each shipment.

a. Prior to taking any action to downgrade or declassify information, the contractor shall seek guidance from the GCA. If such action is approved, all old classification markings shall be canceled and the new markings substituted, whenever practical. In the case of documents, as a minimum the outside of the front cover, the title page, the first page, and the outside of the back shall reflect the new classification markings, or the designation UNCLASSIFIED. Other material shall be re-marked by the most practical method for the type of material involved to ensure that it is clear to the holder what level of classification is assigned to the material.

b. When contractors are notified of downgrading or declassification actions that are contrary to the markings shown on the material, the material shall be re-marked to indicate the change. In addition, the material shall be marked to indicate the authority for the action, the date of the action, and the identity of the person or contractor taking the action. Other holders shall be notified if further dissemination has been made by the contractor.

4-217. Upgrading Action

a. When a notice is received to upgrade material to a higher level, for example from CONFIDENTIAL to SECRET, the new markings shall be immediately entered on the material according to the notice to upgrade, and all the superseded markings shall be obliterated. The authority for and the date of the upgrading action shall be entered on the material. Other holders shall be notified as appropriate if further dissemination of the material has been made by the contractor.

b. The contractor’s notice shall not be classified unless the notice contains additional information warranting classification. In the case of material which was inadvertently released as UNCLASSIFIED, the contractor’s notice shall be classified CONFIDENTIAL, unless it contains additional information warranting a higher classification. The notice shall cite the applicable Contract Security Classification Specification or other classification guide on the "Derived From" line and be marked with an appropriate declassification instruction.

4-218. Inadvertent Release. If classified material is inadvertently distributed outside the facility without the proper classification assigned to it, or without any markings to identify the material as classified, the contractor shall, as appropriate:

a. Determine whether all holders of the material are cleared and authorized access to it.

b. Determine whether control of the material has been lost.

c. If recipients are cleared for access to the material, promptly provide written notice to all holders of the proper classification to be assigned. If control of the material has been lost, if all copies cannot be accounted for, or if unauthorized personnel have had access to it, report the compromise to the CSA.

CHAPTER 5
Safeguarding Classified Information

Section 1. General Safeguarding Requirements

5-100. General. Contractors shall be responsible for safeguarding classified information in their custody or under their control. Individuals are responsible for safeguarding classified information entrusted to them. The extent of protection afforded classified information shall be sufficient to reasonably foreclose the possibility of its loss or compromise.

5-101. Safeguarding Oral Discussions. Contractors shall ensure that all cleared personnel are aware of the prohibition against discussing classified information over unsecured telephones, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

5-102. End of Day Security Checks

a. Contractors that store classified material shall establish a system of security checks at the close of each working day to ensure that all classified material and security repositories have been appropriately secured.

b. Contractors that operate multiple work shifts shall perform the security checks at the end of the last working shift in which classified material was removed from storage for use. The checks are not required during continuous 24-hour operations.

5-103. Perimeter Controls. Contractors authorized to store classified material shall establish and maintain a system to deter and detect unauthorized introduction or removal of classified material from their facility. The objective is to discourage the introduction or removal of classified material without proper authority. If the unauthorized introduction or removal of classified material can be reasonably foreclosed through technical means, which are encouraged, no further controls are necessary. Personnel who have a legitimate need to remove or transport classified material should be provided appropriate authorization for passing through designated entry/exit points. The fact that persons who enter or depart the facility are subject to an inspection of their personal effects shall be conspicuously posted at all pertinent entries and exits.

a. All persons who enter or exit the facility shall be subject to an inspection of their personal effects, except under circumstances where the possibility of access to classified material is remote. Inspections shall be limited to buildings or areas where classified work is being performed. Inspections are not required of wallets, change purses, clothing, cosmetics cases, or other objects of an unusually personal nature.

b. The extent, frequency, and location of inspections shall be accomplished in a manner consistent with contractual obligations and operational efficiency. Inspections may be done using any appropriate random sampling technique. Contractors are encouraged to seek legal advice during the formulation of implementing procedures and to surface significant problems to the CSA.

5-104. Emergency Procedures. Contractors shall develop procedures for safeguarding classified material in emergency situations. The procedures shall be as simple and practical as possible and should be adaptable to any type of emergency that may reasonably arise. Contractors shall promptly report to the CSA any emergency situation that renders the facility incapable of safeguarding classified material.

Section 2. Control and Accountability

5-200. Policy. Contractors shall establish an information management system to protect and control the classified information in their possession. Contractors shall ensure that classified information in their custody is used or retained only for a lawful and authorized U.S. Government purpose. The U.S. Government reserves the right to retrieve its classified material or to cause appropriate disposition of the material by the contractor. The information management system employed by the contractor shall be capable of facilitating such retrieval and disposition in a reasonable period of time.

5-201. Accountability for TOP SECRET

a. TOP SECRET control officials shall be designated to receive, transmit, and maintain access and accountability records for TOP SECRET information. An inventory shall be conducted annually unless written relief is granted by the GCA.

b. The transmittal of TOP SECRET information shall be covered by a continuous receipt system both within and outside the facility.

c. Each item of TOP SECRET material shall be numbered in series. The copy number shall be placed on TOP SECRET documents and on all associated transaction documents.

5-202. Receiving Classified Material. Procedures shall be established to ensure that classified material, regardless of delivery method, is received directly by authorized personnel. The material shall be examined for evidence of tampering and the classified contents shall be checked against the receipt. Discrepancies in the contents of a package or absence of a receipt for TOP SECRET and SECRET material shall be reported promptly to the sender. If the shipment is in order, the receipt shall be signed and returned to the sender. If a receipt is included with CONFIDENTIAL material, it shall be signed and returned to the sender.

5-203. Generation of Classified Material

a. A record of TOP SECRET material produced by the contractor shall be made when the material is: (1) completed as a finished document, (2) retained for more than 30 days after creation, regardless of the stage of development, or (3) transmitted outside the facility.

b. Classified working papers generated by the contractor in the preparation of a finished document shall be: (1) dated when created, (2) marked with its overall classification and with the annotation "WORKING PAPERS", and (3) destroyed when no longer needed. Working papers shall be marked in the same manner prescribed for a finished document at the same classification level when: (1) transmitted outside the facility, or (2) retained for more than 30 days from creation for TOP SECRET, or 180 days from creation for SECRET and CONFIDENTIAL material.

Section 3. Storage and Storage Equipment

5-300. General. This section describes the uniform requirements for the physical protection of classified material in the custody of contractors. Where these requirements are not appropriate for protecting specific types or forms of classified material, compensatory provisions shall be developed and approved by the CSA. Nothing in this manual shall be construed to contradict or inhibit compliance with the law or building codes. Cognizant security officials shall work to meet appropriate security needs according to the intent of this manual and at acceptable cost

5-301. GSA Storage Equipment. GSA establishes and publishes uniform standards, specifications, and supply schedules for units and key-operated and combination padlocks suitable for the storage and protection of classified information. Manufacturers and prices of storage equipment approved by the GSA are listed in the Federal Supply Schedule (P55) catalog (FSC GROUP 71-Pan II). Copies of specifications and schedules may be obtained from any regional office of the GSA.

5-302. TOP SECRET Storage. TOP SECRET material shall be stored in a GSA-approved security container, an approved vault, or an approved closed area with supplemental controls.

5-303. SECRET Storage. SECRET material shall be stored in a GSA-approved security container, an approved vault, or closed area. Supplemental controls are required for storage in closed areas. The following additional storage methods may be used until October 1, 2012:

a. A safe, steel file cabinet, or safe-type steel file container that has an automatic unit locking mechanism. All such receptacles will be accorded supplemental protection during non-working hours.

b. Any steel file cabinet that has four sides and a top and bottom (all permanently attached by welding, rivets or peened bolts so the contents cannot be removed without leaving visible evidence of entry) and is secured by a rigid metal lock bar and an approved key operated or combination padlock. The keepers of the rigid metal lock bar shall be secured to the cabinet by welding, rivets, or bolts so they cannot be removed and replaced without leaving evidence of the entry. The drawers of the container shall be held securely so their contents cannot be removed without forcing open the drawer. This type of cabinet will be accorded supplemental protection during non-working hours.

5-304. CONFIDENTIAL Storage. CONFIDENTIAL material shall be stored in the same manner as TOP SECRET or SECRET material except that no supplemental protection is required.

5-305. Restricted Areas. When it is necessary to control access to classified material in an open area during working hours, a restricted area may be established. A restricted area will normally become necessary when it is impractical or impossible to protect classified material because of its size, quantity or other unusual characteristic. The restricted area shall have a clearly defined perimeter, but physical barriers are not required. Personnel within the area shall be responsible for challenging all persons who may lack appropriate access authority. All classified material will be secured during non-working hours in approved repositories or secured using other methods approved by the CSA.

5-306. Closed Areas. Due to the size and nature of the classified material, or for operational necessity, it may be necessary to construct closed areas for storage because GSA-approved containers or vaults are unsuitable or impractical. Closed areas must be constructed in accordance with section 8 of this chapter. Access to closed areas must be controlled to preclude unauthorized access. This may be accomplished through the use of a cleared person or by a supplanting access control device or system. Access shall be limited to authorized persons who have an appropriate security clearance and a need-to-know for the classified material/information within the area. Persons without the appropriate level of clearance and/or need to know shall be escorted at all times by an authorized person where inadvertent or unauthorized exposure to classified information cannot otherwise be effectively prevented. Closed areas storing TOP SECRET and SECRET material shall be accorded supplemental protection during non-working hours. During non-working hours and during working hours when the area is unattended, admittance to the area shall be controlled by locked entrances and exits secured by either an approved built-in combination lock or an approved combination or key-operated padlock. It is not necessary to activate the supplemental controls during working hours. Doors secured from the inside with a panic bolt (for example, actuated by a panic bar, a dead bolt, a rigid wood or metal bar) or other means approved by the CSA, will

not require additional locking devices.

a. Contractors shall develop and implement procedures to ensure the structural integrity of closed areas above false ceilings and below raised floors.

b. Open shelf or bin storage of SECRET and CONFIDENTIAL documents in closed areas requires CSA approval. For SECRET material only areas protected by an approved Intrusion Detection System (IDS) will qualify for such approval. Open shelf or bin storage of TOP SECRET documents is not permitted.

c. The CSA and the contractor shall agree on the need to establish, and the extent of, closed areas prior to the award of the contract, when possible, or when the need for such areas becomes apparent during contract performance.

d. The CSA may grant self-approval authority to the FSO for closed area approvals provided the FSO meets specified qualification criteria as determined by the CSA.

5-307. Supplemental Protection

a. IDS as described in section 9 of this Chapter shall be used as supplemental protection.

b. Security guards approved as supplemental protection prior to January 1, 1995, may continue to be utilized. When guards are authorized, the schedule of patrol is 2 hours for TOP SECRET material and 4 hours for SECRET material.

c. GSA-approved security containers and approved vaults secured with a locking mechanism meeting Federal Specification FF-L-2740 do not require supplemental protection when the CSA has determined that the GSA-approved security container or approved vault is located in an area of the facility with security-in-depth.

5-308. Protection of Combinations to Security Containers, Cabinets, Vaults and Closed Areas. Only a minimum number of authorized persons shall have knowledge of combinations to authorized storage containers. Containers shall bear no external markings indicating the level of classified material authorized for storage.

a. A record of the names of persons having knowledge of the combination shall be maintained.

b. Security containers, vaults, cabinets, and other authorized storage containers shall be kept locked when not under the direct supervision of an authorized person entrusted with the contents.

c. The combination shall be safeguarded in accordance with the highest classification of the material authorized for storage in the container.

d. If a record is made of a combination, the record shall be marked with the highest classification of material authorized for storage in the container.

5-309. Changing Combinations. Combinations shall be changed by a person authorized access to the contents of the container, or by the FSO or his or her designee. Combinations shall be changed as follows:

a. The initial use of an approved container or lock for the protection of classified material.

b. The termination of employment of any person having knowledge of the combination, or when the clearance granted to any such person has been withdrawn, suspended, or revoked.

c. The compromise or suspected compromise of a container or its combination, or discovery of a container left unlocked and unattended.

d. At other times when considered necessary by the FSO or CSA.

5-310. Supervision of Keys and Padlocks. Use of key-operated padlocks are subject to the following requirements: (i) a key and lock custodian shall be appointed to ensure proper custody and handling of keys and locks used for protection of classified material; (ii) a key and lock control register shall be maintained to identify keys for each lock and their current location and custody; (iii) keys and locks shall be audited each month; (iv) keys shall be inventoried with each change of custody; (v) keys shall not be removed from the premises; (vi) keys and spare locks shall be protected equivalent to the level of classified material involved; (vii) locks shall be changed or rotated at least annually and shall be replaced after loss

or compromise of their operable keys; and (viii) making master keys is prohibited.

5-311. Repair of Approved Containers. Repairs, maintenance, or other actions that affect the physical integrity of a security container approved for storage of classified information shall be accomplished only by appropriately cleared or continuously escorted personnel specifically trained in approved methods of maintenance and repair of containers. Repair procedures may be obtained from the CSA.

a. An approved security container is considered to have been restored to its original state of security integrity if all damaged or altered parts are replaced with manufacturer's replacement or identical cannibalized parts. A signed and dated certification for each repaired container, provided by the repairer, shall be on file setting forth the method of repair used.

b. A container repaired using other than approved methods may be used for storage of SECRET material with supplemental controls only until October 1, 2012.

5-312. Supplanting Access Control Systems or Devices. Automated access control systems and electronic, mechanical, or electromechanical devices which meet the criteria stated in paragraphs 5-313 and 5-314, below, may be used to supplant contractor-authorized personnel or guards to control admittance to closed areas during working hours. Approval of the FSO is required before effecting the installation of a supplanting access control device to meet a requirement of this Manual.

5-313. Automated Access Control Systems. The automated access control system must be capable of identifying the individual entering the area and authenticating that person's authority to enter the area.

a. Manufacturers of automated access control equipment or devices must assure in writing that their system will meet the following standards before FSOs may favorably consider such systems for protection of classified information:

(1) Chances of an unauthorized individual gaining access through normal operation of the equipment are no more than one in ten thousand.

(2) Chances of an authorized individual being rejected for access through normal operation of the equipment are no more than one in one thousand.

b. Identification of individuals entering the area can be obtained by an identification (ID) badge or card, or by personal identity.

(1) The ID badge or card must use embedded sensors, integrated circuits, magnetic stripes or other means of encoding data that identifies the facility and the individual to whom the card is issued.

(2) Personal identity verification identifies the individual requesting access by some unique personal characteristic, such as, (a) fingerprint, (b) hand geometry, (c) handwriting. (d) retina, or (e) voice recognition.

c. In conjunction with an ID badge or card or personal identity verification, a personal identification number (PIN) is required. The PIN must be separately entered into the system by each individual using a keypad device. The PIN shall consist of four or more digits, randomly selected with no known or logical association with the individual. The PIN must be changed when it is believed to have been subjected to compromise.

d. Authentication of the individual's authorization to enter the area must be accomplished within the system by comparing the inputs from the ID badge or card or the personal identity verification device and the keypad with an electronic database of individuals authorized into the area. A procedure must be established for removal of the individual's authorization to enter the area upon reassignment, transfer or termination, or when the individual's PCL is suspended or revoked.

e. Locations where access transactions are, or can be displayed, and where authorization data, card encoded data and personal identification or verification data is input, stored, displayed, or recorded must be protected.

f. Control panels, card readers, keypads, communication or interface devices located outside the entrance to a closed area shall have tamper-resistant enclosures, be securely fastened to a wall or other structure, be protected by a tamper alarm, or secured with an approved combination padlock. Control panels located within a closed area shall require only a

minimal degree of physical security protection sufficient to preclude unauthorized access to the mechanism. Where areas containing TOP SECRET information are involved, tamper alarm protection is mandatory.

g. Systems that utilize transmission lines to carry access authorization, personal identification, or verification data between devices/equipment located outside the closed area shall receive circuit protection equal to or greater than that specified as Grade A by Underwriters Laboratories (UL).

h. Access to records and information concerning encoded ID data and PINs shall be restricted to individuals cleared at the same level as the highest classified information contained within the specific area or areas in which ID data or PINs are utilized. Access to identification or authorization data, operating system software or any identifying data associated with the access control system shall be limited to the least number of personnel possible. Such data or software shall be kept secured when unattended.

i. Records reflecting active assignments of ID badges/cards, PINs, levels of access, and similar system-related records shall be maintained. Records concerning personnel removed from the system shall be retained for 90 days.

j. Personnel entering or leaving an area shall be required to immediately secure the entrance or exit point. Authorized personnel who permit another individual entrance into the area are responsible for confirming the individual's PCL and need-to-know. During shift changes and emergency situations, if the door remains open, admittance shall be controlled by a contractor-authorized person or guard stationed to supervise the entrance to the area.

5-314. Electronic, Mechanical, or Electro-mechanical Devices. Provided the classified material within the closed area is no higher than SECRET, electronic, mechanical, or electro-mechanical devices that meet the criteria below may be used to supplant contractor authorized personnel or guards to control admittance to closed areas during working hours. Devices may be used that operate by either a push-button combination that activates the locking device or by a control card used in conjunction with a push-button combination, thereby excluding any system that operates solely by the use of a control card.

a. The electronic control panel containing the mechanism by which the combination is set may be located inside or outside the closed area. When located outside the closed area, the control panel shall be securely fastened or attached to the perimeter barrier of the area and secured by an approved combination padlock. If the control panel is located within the closed area, it shall require only a minimal degree of physical security designed to preclude unauthorized access to the mechanism.

b. The control panel shall be installed in a manner that precludes an unauthorized person in the immediate vicinity from observing the selection of the correct combination of the push buttons, or have a shielding device mounted.

c. The selection and setting of the combination shall be accomplished by an employee of the contractor who is authorized to enter the area. The combination shall be changed as specified in paragraph 5-309. The combination shall be classified and safeguarded in accordance with the classification of the highest classified material within the closed area.

d. Electrical gear, wiring included, or mechanical links (cables, rods, etc.) shall be accessible only from inside the area, or shall be secured within a protective covering to preclude surreptitious manipulation of components.

e. Personnel entering or leaving the area shall be required to secure the entrance or exit point immediately. Authorized personnel who permit another individual entrance into the area are responsible for confirming the individual's PCL and need-to-know. During shift changes and emergency situations, if the door remains open, admittance shall be controlled by a contractor-authorized person or guard stationed to supervise the entrance to the area.

Section 4. Transmission

5-400. General. Classified material shall be transmitted outside the contractor's facility in a manner that prevents loss or unauthorized access.

5-401. Preparation and Receipting

a. Classified information to be transmitted outside of a facility shall be enclosed in opaque inner and outer covers. The inner cover shall be a sealed wrapper or envelope plainly marked with the assigned classification and addresses of both sender and addressee. The outer cover shall be sealed and addressed with no identification of the classification of its contents. A receipt shall be attached to or enclosed in the inner cover, except that CONFIDENTIAL information shall require a receipt only if the sender deems it necessary. The receipt shall identify the sender, the addressee and the document, but shall contain no classified information. It shall be signed by the recipient and returned to the sender.

b. A suspense system will be established to track transmitted documents until a signed copy of the receipt is returned.

c. When the material is of a size, weight, or nature that precludes the use of envelopes, the materials used for packaging shall be of such strength and durability to ensure the necessary protection while the material is in transit.

5-402. TOP SECRET Transmission Outside a Facility. Written authorization of the GCA is required to transmit TOP SECRET information outside of the facility. TOP SECRET material may be transmitted by the following methods within and directly between the United States and its territorial areas.

a. The Defense Courier Service, if authorized by the GCA.

b. A designated courier or escort cleared for access to TOP SECRET information.

c. By electrical means over CSA-approved secured communications security circuits, provided such transmission conforms with this Manual, the telecommunications security provisions of the contract, or as otherwise authorized by the GCA.

5-403. SECRET Transmission Outside a Facility. SECRET material may be transmitted by one of the following methods within and directly between the United States and its territorial areas:

a. By the methods established for TOP SECRET.

b. U.S. Postal Service Express Mail and U.S. Postal Service Registered Mail. NOTE: The "Waiver of Signature and Indemnity" block on the U.S. Postal Service Express Mail Label 11-B may not be executed and the use of external (street side) express mail collection boxes is prohibited.

c. A cleared commercial carrier.

d. A cleared commercial messenger service engaged in the intracity/local area delivery (same day delivery only) of classified material.

e. A commercial delivery company, approved by the CSA, that provides nation-wide, overnight service with computer tracking and reporting features. Such companies need not be security cleared.

f. Other methods as directed in writing by the GCA.

5-404. CONFIDENTIAL Transmission Outside a Facility. CONFIDENTIAL material shall be transmitted by the methods established for SECRET material, except that a commercial carrier does not have to be cleared, or by U.S. Postal Service Certified Mail.

5-405. Transmission Outside the United States and Its Territorial Areas. Classified material may be transmitted to a U.S. Government activity outside the United States or a U.S. territory only under the provisions of a classified contract or with the written authorization of the GCA.

a. TOP SECRET material may be transmitted by the Defense Courier Service, Department of State Courier System, or a courier service authorized by the GCA.

b. SECRET and CONFIDENTIAL material may be transmitted by: (1) registered mail through U.S. Army, Navy, or Air Force postal facilities; (2) by an appropriately cleared contractor employee; (3) by a U.S. civil service employee or military person, who has been designated by the GCA; (4) by U.S. and Canadian registered mail with registered mail receipt

to and from Canada and via a U.S. or a Canadian government activity; or (5) as authorized by the GCA.

5-406. Addressing Classified Material. Mail or shipments containing classified material shall be addressed to the Commander or approved classified mailing address of a Federal activity or to a cleared contractor using the name and classified mailing address of the facility. An individual's name shall not appear on the outer cover. This does not prevent the use of office code letters, numbers, or phrases in an attention line to aid in internal routing.

a. When it is necessary to direct SECRET or CONFIDENTIAL material to the attention of a particular individual, other than as prescribed below, the identity of the intended recipient shall be indicated on an attention line placed in the letter of transmittal or on the inner container or wrapper.

b. When addressing SECRET or CONFIDENTIAL material to an individual operating as an independent consultant, or to any facility at which only one employee is assigned, the outer container shall specify: "TO BE OPENED BY ADDRESSEE ONLY" and be annotated: "POSTMASTER-DO NOT FORWARD. IF UNDELIVERABLE TO ADDRESSEE, RETURN TO SENDER."

5-407. Transmission Within a Facility. Classified material may be transmitted within a facility without single or double-wrapping provided adequate measures are taken to protect the material against unauthorized disclosure.

5-408. SECRET Transmission by Commercial Carrier. SECRET material may be shipped by a cleared commercial carrier that has been approved by the CSA to transport SECRET shipments. Commercial carriers may be used only within and between the 48 contiguous States and the District of Columbia or wholly within Alaska, Hawaii, or a U.S. territory. When the services of a commercial carrier are required, the contractor, as consignor, shall be responsible for the following:

a. The material shall be prepared for transmission to afford additional protection against pilferage, theft, and compromise as follows.

(1) The material shall be shipped in hardened containers unless specifically authorized otherwise by the contracting agency.

(2) Carrier equipment shall be sealed by the contractor or a representative of the carrier when there is a full carload, a full truckload, exclusive use of the vehicle, or when a closed and locked compartment of the carrier's equipment is used. The seals shall be numbered and the numbers indicated on all copies of the bill of lading (BL). When seals are used, the BL shall be annotated substantially as follows: DO NOT BREAK SEALS EXCEPT IN CASE OF EMERGENCY OR UPON PRIOR AUTHORITY OF THE CONSIGNOR OR CONSIGNEE. IF FOUND BROKEN OR IF BROKEN FOR EMERGENCY REASONS, APPLY CARRIER'S SEALS AS SOON AS POSSIBLE AND IMMEDIATELY NOTIFY BOTH THE CONSIGNOR AND THE CONSIGNEE.

(3) For DoD contractors the notation "Protective Security Service Required" shall be reflected on all copies of the BL. The BL will be maintained in a suspense file to follow-up on overdue or delayed shipments.

b. The contractor shall utilize a qualified carrier selected by the U.S. Government that will provide a single-line service from point of origin to destination, when such service is available, or by such transshipping procedures as may be specified by the U.S. Government.

c. The contractor shall request routing instructions, including designation of a qualified carrier, from the GCA or designated representative (normally the government transportation officer). The request shall specify that the routing instructions are required for the shipment of SECRET material and include the point of origin and point of destination.

d. The contractor shall notify the consignee (including U.S. Government transshipping activity) of the nature of the shipment, the means of the shipment, numbers of the seals, if used, and the anticipated time and date of arrival by separate communication at least 24 hours in advance (or immediately on dispatch if transit time is less than 24 hours) of the arrival of the shipment. This notification shall be addressed to the appropriate organizational entity and not to an individual. Request that the consignee activity (including a military transshipping activity) notify the consignor of any shipment not received within 48 hours after the estimated time of arrival indicated by the consignor.

e. In addition, the contractor shall annotate the BL: "CARRIER TO NOTIFY THE CONSIGNOR AND CONSIGNEE (Telephone Numbers) IMMEDIATELY IF SHIPMENT IS DELAYED

BECAUSE OF AN ACCIDENT OR INCIDENT. IF NEITHER CAN BE REACHED, CONTACT (Enter appropriate HOTLINE Number). USE HOTLINE NUMBER TO OBTAIN SAFE HAVEN OR REFUGE INSTRUCTIONS IN THE EVENT OF A CIVIL DISORDER, NATURAL DISASTER, CARRIER STRIKE OR OTHER EMERGENCY."

5-409. CONFIDENTIAL Transmission by Commercial Carrier. CONFIDENTIAL material may be shipped by a CSA or GCA-approved commercial carrier. For DoD contractors a commercial carrier authorized by law, regulatory body, or regulation to provide the required transportation service shall be used when a determination has been made by the Surface Deployment and Distribution Command (SDDC) (formerly known as the Military Traffic Management Command) that the carrier has a tariff, government tender, agreement, or contract that provides Constant Surveillance Service. Commercial carriers may be used only within and between the 48 contiguous states and the District of Columbia or wholly within Alaska, Hawaii, or a U.S. territory. An FCL is not required for the commercial carrier. The contractor, as consignor, shall:

a. Utilize containers of such strength and durability as to provide security protection to prevent items from breaking out of the container and to facilitate the detection of any tampering with the container while in transit;

b. For DoD contractors indicate on the BL, "Constant Surveillance Service Required." In addition, annotate the BL as indicated in 5-408e.

c. Instruct the carrier to ship packages weighing less than 200 pounds gross in a closed vehicle or a closed portion of the carrier's equipment.

5-410. Use of Couriers, Handcarriers, and Escorts. Contractors who designate cleared employees as couriers, handcarriers, and escorts shall ensure:

a. They are briefed on their responsibility to safeguard classified information.

b. They possess an identification card or badge which contains the contractor's name and the name and a photograph of the employee.

c. The employee retains classified material in his or her personal possession at all times. Arrangements shall be made in advance of departure for overnight storage at a U.S. Government installation or at a cleared contractor's facility that has appropriate storage capability, if needed.

d. If the classified material is being handcarried to a classified meeting or on a visit, an inventory of the material shall be made prior to departure. A copy of the inventory shall be carried by the employee. On the employee's return to the facility, an inventory shall be made of the material for which the employee was charged.

5-411. Use of Commercial Passenger Aircraft for Transmitting Classified Material. Classified material may be handcarried aboard commercial passenger aircraft by cleared employees with the approval of the FSO.

a. **Routine Processing.** Employees handcarrying classified material will be subject to routine processing by airline security agents. Hand-held packages will normally be screened by x-ray examination. If security personnel are not satisfied with the results of the inspection, and the prospective passenger is requested to open a classified package for visual examination the traveler shall inform the screener that the carry-on items contain U.S. Government classified information and cannot be opened. Under no circumstances may the classified material be opened by the traveler or security personnel.

b. **Special Processing.** When routine processing would subject the classified material to compromise or damage; when visual examination is or may be required to successfully screen a classified package; or when classified material is in specialized containers which due to its size, weight, or other physical characteristics cannot be routinely processed, the contractor shall contact the appropriate air carrier in advance to explain the particular circumstances and obtain instructions on the special screening procedures to be followed.

c. **Authorization Letter.** Contractors shall provide employees with written authorization to handcarry classified material on commercial aircraft. The written authorization shall:

(1) Provide the full name, date of birth, height, weight, and signature of the traveler and state that he or she is authorized to transmit classified material;

(2) Describe the type of identification the traveler will present on request;

(3) Describe the material being handcarried and request that it be exempt from opening;

(4) Identify the points of departure, destination, and known transfer points;

(5) Include the name, telephone number, and signature of the FSO, and the location and telephone number of the CSA.

5-412. Use of Escorts for Classified Shipments. If an escort is necessary to ensure the protection of the classified information being transported, a sufficient number of escorts shall be assigned to each classified shipment to ensure continuous surveillance and control over the shipment while in transit. Specific written instructions and operating procedures shall be furnished escorts prior to shipping and shall include the following:

a. Name and address of persons, including alternates, to whom the classified material is to be delivered;

b. Receipting procedures;

c. Means of transportation and the route to be used;

d. Duties of each escort during movement, during stops en route, and during loading and unloading operations; and

e. Emergency and communication procedures.

5-413. Functions of an Escort. Escorts shall be responsible for the following.

a. Accept custody for the shipment by signing a receipt and release custody of the shipment to the consignee after obtaining a signed receipt.

b. When accompanying a classified shipment in an express or freight car, provide continuous observation of the containers and observe adjacent areas during stops or layovers.

c. When traveling in an escort car accompanying a classified shipment via rail, keep the shipment cars under observation and detrain at stops, when practical and time permits, in order to guard the shipment cars and check the cars or containers locks and seals. The escort car (after arrangements with the railroad) should be pre-positioned immediately behind the car used for the classified shipment to enable the escort to keep the shipment car under observation.

d. Maintain liaison with train crews, other railroad personnel, special police, and law enforcement agencies, as necessary.

e. When escorting classified shipments via motor vehicles, maintain continuous vigilance for the presence of conditions or situations that might threaten the security of the cargo, take such action as circumstances might require to avoid interference with continuous safe passage of the vehicle, check seals and locks at each stop where time permits, and observe vehicles and adjacent areas during stops or layovers.

f. When escorting shipments via aircraft, provide continuous observation of plane and cargo during ground stops and of cargo during loading and unloading operations. The escort shall not board the plane until after the cargo area is secured. Furthermore, the escort should preferably be the first person to depart the plane to observe the opening of the cargo area. Advance arrangements with the airline are required.

g. Notify the consignor by the fastest means available if there is an unforeseen delay en route, an alternate route is used, or an emergency occurs. If appropriate and the security of the shipment is involved, notify the nearest law enforcement official.

Section 5. Disclosure

5-500. General. Contractors shall ensure that classified information is disclosed only to authorized persons.

5-501. Disclosure to Employees. Contractors are authorized to disclose classified information to their cleared employees as necessary for the performance of tasks or services essential to the fulfillment of a classified contract or subcontract.

5-502. Disclosure to Subcontractors. Contractors are authorized to disclose classified information to a cleared subcontractor when access is necessary for the performance of tasks or services essential to the fulfillment of a prime contract or a subcontract.

5-503. Disclosure between Parent and Subsidiaries. Disclosure of classified information between a parent and its subsidiaries, or between subsidiaries, shall be accomplished in the same manner as prescribed in 5-502 for subcontractors.

5-504. Disclosure in an MFO. Disclosure of classified information between cleared facilities of the MFO shall be accomplished in the same manner as prescribed in 5-501 for employees.

5-505. Disclosure to DoD Activities. Contractors are authorized to disclose classified information received or generated under a DoD classified contract to another DoD activity unless specifically prohibited by the DoD activity that has classification jurisdiction over the information.

5-506. Disclosure to Federal Agencies. Contractors shall not disclose classified information received or generated under a contract from one agency to any other Federal agency unless specifically authorized by the agency that has classification jurisdiction over the information.

5-507. Disclosure of Classified Information to Foreign Persons. Contractors shall not disclose classified information to foreign persons unless release of the information is authorized in writing by the Government Agency having classification jurisdiction over the information involved, e.g. the DOE for RD and FRD, the NSA for COMSEC, the DNI for SCI, and all other Executive Branch departments and agencies for classified information under their jurisdiction. The disclosure must also be consistent with applicable U.S. laws and regulations.

5-508. Disclosure of Export Controlled Information to Foreign Persons. Contractors shall not disclose export-controlled information and technology (classified or unclassified) to a foreign person, whether an employee or not, or whether disclosure occurs in the United States or abroad, unless such disclosure is in compliance with applicable U.S. laws and regulations.

5-509. Disclosure to Other Contractors. Contractors shall not disclose classified information to another contractor except in furtherance of a contract, subcontract, or other GCA purpose.

5-510. Disclosure of Classified Information in Connection with Litigation. Contractors shall not disclose classified information to attorneys hired solely to represent the contractor in any civil or criminal case in Federal or state courts unless the disclosure is specifically authorized by the agency that has jurisdiction over the information. Contractors shall not disclose classified information to any Federal or state court except on specific instructions of the agency which has jurisdiction over the information or the attorney representing the United States in the case. (For criminal cases in Federal courts, see paragraph 1-208.)

5-511. Disclosure to the Public. Contractors shall not disclose classified or unclassified information pertaining to a classified contract to the public without prior review and clearance as specified in the Contract Security Classification Specification for the contract or as otherwise specified by the GCA.

a. Requests for approval shall be submitted through the activity specified in the GCA-provided classification guidance for the contract involved. Each request shall indicate the approximate date the contractor intends to release the information for public disclosure and identify the media to be used for the initial release. A copy of each approved request for release shall be retained for a period of one inspection cycle for review by the CSA. All information developed subsequent to the initial approval shall also be cleared by the appropriate office prior to public disclosure.

b. The following information need not be submitted for approval unless specifically prohibited by the GCA:

(1) The fact that a contract has been received, including the subject matter of the contract and/or type

of item in general terms provided the name or description of the subject matter is not classified.

(2) The method or type of contract; such as, bid, negotiated, or letter.

(3) Total dollar amount of the contract unless that information equates to (a) a level of effort in a sensitive research area, or (b) quantities of stocks of certain weapons and equipment that are classified.

(4) Whether the contract will require the hiring or termination of employees.

(5) Other information that from time-to-time may be authorized on a case-by-case basis in a specific agreement with the contractor.

(6) Information previously officially approved for public disclosure.

c. The procedures of this paragraph also apply to information pertaining to classified contracts intended for use in unclassified brochures, promotional sales literature, reports to stockholders, or similar material.

d. Information that has been declassified is not automatically authorized for public disclosure. Contractors shall request approval for public disclosure of "declassified" information in accordance with the procedures of this paragraph.

Section 6. Reproduction

5-600. General. Contractors shall establish a control system to ensure that reproduction of classified material is held to the minimum consistent with contractual and operational requirements. Classified reproduction shall be accomplished by authorized personnel knowledgeable of the procedures. The use of technology that prevents, discourages, or detects the unauthorized reproduction of classified documents is encouraged.

5-601. Limitations

a. TOP SECRET documents may be reproduced as necessary in the preparation of a contract deliverable. Reproduction for any other purpose requires the consent of the GCA.

b. Unless restricted by the GCA, SECRET and CONFIDENTIAL documents may be reproduced as follows:

(1) Performance of a prime contract or a subcontract in furtherance of a prime contract.

(2) Preparation of a solicited or unsolicited bid, quotation, or proposal to a Federal agency or prospective subcontractor.

(3) Preparation of patent applications to be filed in the U.S. Patent Office.

c. Reproduced copies of classified documents shall be subject to the same protection as the original documents.

5-602. Marking Reproductions. All reproductions of classified material shall be conspicuously marked with the same classification markings as the material being reproduced. Copies of classified material shall be reviewed after the reproduction process to ensure that these markings are visible.

5-603. Records. Contractors shall maintain a record of the reproduction of all TOP SECRET material for 2 years.

Section 7. Disposition and Retention

5-700. General

a. Classified information no longer needed shall be processed for appropriate disposition. Classified information approved for destruction shall be destroyed in accordance with this section. The method of destruction must preclude recognition or reconstruction of the classified information or material.

b. Contractors shall establish procedures for review of their classified holdings on a recurring basis to reduce these classified inventories to the minimum necessary for effective and efficient operations. Multiple copies, obsolete material, and classified waste shall be destroyed as soon as practical after it has served its purpose. Any appropriate downgrading and declassification actions shall be taken on a timely basis to reduce the volume and to lower the level of classified material being retained by the contractor.

5-701. Retention of Classified Material. Contractors are authorized to retain classified material received or generated under a contract for a period of 2 years after completion of the contract, provided the GCA does not advise to the contrary. If retention is required beyond the 2-year period, the contractor must request and receive written retention authority from the GCA.

a. Contractors shall identify classified material for retention beyond 2 years as follows:

(1) TOP SECRET material shall be identified in a list of specific documents unless the GCA authorizes identification by subject matter and approximate number of documents.

(2) SECRET and CONFIDENTIAL material may be identified by general subject matter and the approximate number of documents.

b. Contractors shall include a statement of justification for retention based on the following:

(1) The material is necessary for the maintenance of the contractor's essential records.

(2) The material is patentable or proprietary data to which the contractor has title.

(3) The material will assist the contractor in independent research and development efforts.

(4) The material will benefit the U.S. Government in the performance of other prospective or existing agency contracts.

(5) The material will benefit the U.S. Government in the performance of another active contract and will be transferred to that contract (specify contract).

c. If retention beyond 2 years is not authorized, all classified material received or generated in the performance of a classified contract shall be destroyed unless it has been declassified or the GCA has requested that the material be returned.

5-702. Termination of Security Agreement. Notwithstanding the provisions for retention outlined above, in the event that the FCL is to be terminated, the contractor shall return all classified material in its possession to the GCA concerned, or dispose of such material in accordance with instructions from the CSA.

5-703. Disposition of Classified Material Not Received Under a Specific Contract.

a. Contractors shall return or destroy classified material received with a bid, proposal, or quote in accordance with the following schedule:

(1) If a bid, proposal, or quote is not submitted or is withdrawn within 180 days after the opening date of bids, proposals, or quotes.

(2) If a bid, proposal, or quote is not accepted within 180 days after notification that a bid, proposal, or quote has not been accepted.

b. If the classified material was not received under a specific contract, such as material obtained at classified meetings or from a secondary distribution center, within 1 year after receipt.

5-704. Destruction. Contractors shall destroy classified material in their possession as soon as possible after it has served the purpose for which it was released by the government, developed or prepared by the contractor, or retained after completion or termination of the contract.

5-705. Methods of Destruction. Classified material may be destroyed by burning, shredding, pulping, melting, mutilation, chemical decomposition, or pulverizing (for example, hammer mills, choppers, and

hybridized disintegration equipment). Pulpers, pulverizers, or shredders may be used only for the destruction of paper products. High wet strength paper, paper mylar, durable-medium paper substitute, or similar water repellent papers are not sufficiently destroyed by pulping; other methods such as disintegration, shredding, or burning shall be used to destroy these types of papers. Residue shall be inspected during each destruction to ensure that classified information cannot be reconstructed. Crosscut shredders currently in use capable of maintaining a shred size not exceeding 1/32 inch in width (with a 1/64 inch tolerance by 1/2 inch in length) may continue to be used. However, any crosscut shredders requiring replacement of the unit and/or rebuilding of the shredder blades assembly must be replaced by a crosscut shredder on the latest NSA Evaluated Products List of High Security Crosscut Shredders. The list may be obtained from the CSA. Classified material in microform; that is, microfilm, microfiche, or similar high data density material; may be destroyed by burning or chemical decomposition, or other methods as approved by the CSA.

a. Public destruction facilities may be used only with the approval of, and under conditions prescribed by, the CSA.

b. Classified material removed from a cleared facility for destruction shall be destroyed on the same day it is removed.

5-706. Witness to Destruction. Classified material shall be destroyed by authorized personnel who have a full understanding of their responsibilities. For destruction of TOP SECRET material, two persons are required. For destruction of SECRET and CONFIDENTIAL material, one person is required.

5-707. Destruction Records. Destruction records are required for TOP SECRET material. The records shall indicate the date of destruction, identify the material destroyed, and be signed by the individuals designated to destroy and witness the destruction. Destruction officials shall be required to know, through their personal knowledge, that such material was destroyed. At the contractor's discretion, the destruction information required may be combined with other required control records. Destruction records shall be maintained by the contractor for 2 years.

5-708. Classified Waste. Classified waste shall be destroyed as soon as practical. This applies to all waste material containing classified information. Pending destruction, classified waste shall be safeguarded as required for the level of classified material involved. Receptacles utilized to accumulate classified waste shall be clearly identified as containing classified material.

Section 8. Construction Requirements

5-800. General. This section describes the construction requirements for closed areas and vaults. Construction shall conform to the requirements of this section or, with CSA approval, to the standards of DCID 6/9 (reference (o)).

5-801. Construction Requirements for Closed Areas. This paragraph specifies the minimum safeguards and standards required for the construction of closed areas that are approved for use for safeguarding classified material. These criteria and standards apply to all new construction and reconstruction, alterations, modifications, and repairs of existing areas. They will also be used for evaluating the adequacy of existing areas.

a. **Hardware.** Only heavy-gauge hardware shall be used in construction. Hardware accessible from outside the area shall be peened, pinned, brazed, or spot welded to preclude removal.

b. **Walls.** Construction may be of material offering resistance to, and evidence of, unauthorized entry into the area. If insert-type panels are used, a method shall be devised to prevent the removal of such panels without leaving visual evidence of tampering. If visual access is a factor, area barrier walls up to a height of 8 feet shall be of opaque or translucent construction.

c. **Windows.** Windows that can be opened and that are less than 18 feet from an access point (for example, another window outside the area, roof, ledge, or door) shall be fitted with 1/2-inch bars (separated by no more than 6 inches), plus crossbars to prevent spreading, 18-gauge expanded metal or wire mesh securely fastened on the inside. When visual access of classified information is a factor, the windows shall be covered by any practical method, such as drapes, blinds, or paint covering the inside of the glass. During nonworking hours, the windows shall be closed and securely fastened to preclude surreptitious entry.

d. **Doors.** Doors shall be constructed of material offering resistance to and detection of unauthorized entry. When windows, louvers, baffle plates, or similar openings are used, they shall be secured with 18-gauge expanded metal or with wire mesh securely fastened on the inside. If visual access is a factor, the windows shall be covered. When doors are used in pairs, an astragal (overlapping molding) shall be installed where the doors meet.

e. **Door Locking Devices.** Entrance doors shall be secured with either an approved built-in combination lock, an approved combination padlock, or with an approved key-operated padlock. Other doors shall be secured from the inside with a panic bolt (for example, actuated by a panic bar); a dead bolt; a rigid wood or metal bar (which shall preclude "springing") which extends across the width of the door and is held in position by solid clamps, preferably on the door casing; or by other means approved by the CSA consistent with relevant fire and safety codes.

f. **Ceilings.** Ceilings shall be constructed of material offering resistance to and detection of unauthorized entry. Wire mesh or other non-opaque material offering similar resistance to, and evidence of, unauthorized entry into the area may be used if visual access to classified material is not a factor.

g. **Ceilings (Unusual Cases).** When wall barriers do not extend to the true ceiling and a false ceiling is created, the false ceiling must be reinforced with wire mesh or 18-gauge expanded metal to serve as the true ceiling. When wire mesh or expanded metal is used, it must overlap the adjoining walls and be secured in a manner that precludes removal without leaving evidence of tampering. When wall barriers of an area do extend to the true ceiling and a false ceiling is added, there is no necessity for reinforcing the false ceiling. When there is a valid justification for not erecting a solid ceiling as part of the area, such as the use of overhead cranes for the movement of bulky equipment within the area, the contractor shall ensure that surreptitious entry cannot be obtained by entering the area over the top of the barrier walls.

h. **Miscellaneous Openings.** All vents, ducts and similar openings into closed areas that measure in excess of 96 square inches and over 6 inches in their smallest dimension must be protected with either ½-inch diameter steel bars with a maximum space of 6 inches between the bars; grills consisting of 18-gauge expanded metal, wire mesh; or an equivalent gauge commercial metal duct barrier. The barriers must be secured to preclude removal from outside the area, and the method of installation must ensure that classified material cannot be removed through the openings with the aid of any type of instrument. A barrier will not be required if an approved IDS provides protection of the opening.

5-802. Construction Required for Vaults. This paragraph specifies the minimum standards required

for the construction of vaults approved for use as storage facilities for classified material. These standards apply to all new construction and reconstruction, alterations, modifications, and repairs of existing vaults. They will also be used for evaluating the adequacy of existing vaults. In addition to the requirements given below, the wall, floor, and roof construction shall be in accordance with nationally recognized standards of structural practice. For the vaults described below, the concrete shall be poured in place and will have a compressive strength of 2,500 pounds per square inch.

a. **Floor.** The floor must be a monolithic concrete construction of the thickness of adjacent concrete floor construction, but not less than 4 inches thick.

b. **Walls.** Walls must be not less than 8-inch-thick hollow clay tile (vertical cell double shells) or concrete blocks (thick shells). Monolithic steel-reinforced concrete walls at least 4 inches thick may also be used. Where hollow clay tiles are used and such masonry units are flush, or in contact with, facility exterior walls, they shall be filled with concrete and steel-reinforced bars. Walls are to extend to the underside of the roof or ceiling above.

c. **Roof/Ceiling.** The roof or ceiling must be a monolithic reinforced concrete slab of a thickness to be determined by structural requirements.

d. **Vault Door and Frame Unit.** A GSA-approved vault door and frame unit shall be used.

e. **Miscellaneous Openings.** Omission of all miscellaneous openings is desirable, but not mandatory. Openings of such size and shape as to permit unauthorized entry, (normally in excess of 96 square inches in area and over 6 inches in its smallest dimension) and openings for ducts, pipes, registers, sewers and tunnels shall be equipped with man-safe barriers such as wire mesh, 18-gauge expanded metal, or rigid metal bars of at least 1/2 inch in diameter extending across their width with a maximum space of 6 inches between the bars. The rigid metal bars shall be securely fastened at both ends to preclude removal and, if the bars exceed 18 inches in length, shall have crossbars to prevent spreading. Where wire mesh, expanded metal, or rigid metal bars are used, care shall be exercised to ensure that classified material within the vault cannot be removed with the aid of any type of instrument. Pipes and conduits entering the vault shall enter through walls that are not common to the vault and the structure housing the vault. Preferably such pipes and conduits should be installed when the vault is constructed. If this is not practical, they shall be carried through snug-fitting pipe sleeves cast in the concrete. After installation, the annular space between the sleeve and the pipe or conduit shall be caulked solid with lead, wood, waterproof (silicone) caulking, or similar material, which will give evidence of surreptitious removal.

Section 9. Intrusion Detection Systems

5-900. General. This section specifies the minimum standards for an approved IDS when supplemental protection is required for TOP SECRET and SECRET material. The IDS shall be connected to, and monitored by, a central monitoring station. Alarm system installation shall conform to the requirements of this section or to the standards set forth in reference (o). The CSA will approve contingency protection procedures in the event of IDS malfunction.

5-901. CSA Approval

a. CSA approval is required before installing an IDS. Approval of a new IDS shall be based on the criteria of reference (o) or UL Standard 2050, reference (p), as determined by the CSA.

b. The UL listed Alarm Service Company (ASC) is responsible for completing the Alarm System Description Form.

5-902. Central Monitoring Station

a. The central monitoring station may be located at a UL-listed: (1) Government Contractor Monitoring Station (GCMS), formerly called a proprietary central station; (2) cleared commercial central station; (3) cleared protective signal service station (e.g., fire alarm monitor); or (4) cleared residential monitoring station. For the purpose of monitoring alarms, all provide an equivalent level of monitoring service.

b. SECRET-cleared central station employees shall be in attendance at the alarm monitoring station in sufficient number to monitor each alarmed area within the cleared contractor facility.

c. The central monitoring station shall be required to indicate whether or not the system is in working order and to indicate tampering with any element of the system. Necessary repairs shall be made as soon as practical. Until repairs are completed, periodic patrols shall be conducted during non-working hours, unless a SECRET cleared employee is stationed at the alarmed site.

d. When an IDS is used, it shall be activated immediately at the close of business at the alarmed area or container. This may require that the last person who departs the controlled area or checks the security container notify the central monitoring station to set the alarm. A record shall be maintained to identify the person responsible for setting and deactivating the IDS. Each failure to activate or deactivate shall be reported to the FSO. Such records shall be maintained for 30 days.

e. Records shall be maintained for 90 days indicating time of receipt of alarm, name(s) of security force personnel responding, time dispatched to facility/area, time security force personnel arrived, nature of alarm, and what follow-up actions were accomplished.

5-903. Investigative Response to Alarms. The primary purpose of any alarm response team is to ascertain if intrusion has occurred and if possible assist in the apprehension of the individuals involved. If an alarm activation resets in a reasonable amount of time and no damage to the area or container is visible, then entrance into the area or container is not required. Therefore, the initial response team may consist of uncleared personnel. If the alarm activation does not reset and damage is observed, then a cleared response team must be dispatched. The initial uncleared response team must stay on station until relieved by the cleared response team. If a cleared response team does not arrive within one hour, then a report to the CSA must be made by the close of the next business day.

a. The following resources may be used to investigate alarms: proprietary security force personnel, central station guards, or a subcontracted guard service.

(1) For a GCMS, trained proprietary or subcontractor security force personnel, cleared to the SECRET level and sufficient in number to be dispatched immediately to investigate each alarm, shall be available at all times when the IDS is in operation.

(2) For a commercial central station, protective signaling service station, or residential monitoring station, there shall be a sufficient number of trained guards available to respond to alarms. Guards shall be cleared only if they have the ability and responsibility to access the area or container(s) housing classified material; i.e., keys to the facility have been provided or the personnel are authorized to enter the building or check the container or area that contains classified material.

(3) Uncleared guards dispatched by a commercial central station, protective signaling service station, or residential monitoring station in response to an alarm shall remain on the premises until a

designated, cleared representative of the facility arrives, or for a period of not less than 1 hour, whichever comes first. If a cleared representative of the facility does not arrive within 1 hour following the arrival of the guard, the central control station must provide the CSA with a report of the incident that includes the name of the subscriber facility, the date and time of the alarm, and the name of the subscriber's representative who was contacted to respond. A report shall be submitted to the CSA within 24 hours of the next working day.

(4) Subcontracted guards must be under a classified contract with either the installing alarm company or the cleared facility.

b. The response time shall not exceed 15 minutes. When environmental factors (e.g., traffic, distance) legitimately prevent a 15-minute response time, the CSA may authorize up to a 30-minute response time. The CSA approval shall be documented on the UL Alarm System Description Form and the specified response time shall be noted on the alarm certificate. The UL standard for response within the time limits is 80%. That is the minimum allowable on-time response rate and anything less than 80% is unacceptable. However, in all cases, a guard or cleared employee must arrive at the alarmed premises.

5-904. Installation. The IDS at the facility, area or container shall be installed by a UL listed ASC or by a company approved by the CSA. When connected to a commercial central station, GCMS protective signaling service or residential monitoring station, the service provided shall include line security (i.e., the connecting lines are electronically supervised to detect evidence of tampering or malfunction), the extent of protection for a container shall be "Complete," and for an alarmed area shall be "Extent 3" as described in the reference (p) installation guide. CSA authorization on the Alarm System Description Form is required in the following circumstances:

a. Line security is not available. Installation will require two independent means of transmission of the alarm signal from the alarmed area to the monitoring station.

b. Alarm installation provides Extent 5 Protection. Reference (p) allows for Extent 5 based on patrolling guards and CSA approval of security-in-depth.

c. Law enforcement personnel are the primary alarm response. The contractor must obtain written assurance from the police department regarding the ability to respond to alarms.

d. Alarm signal transmission is over computer controlled data-networks (internet, intranet, etc.). The CSA will provide specific acceptance criteria (e.g., encryption requirements, etc.) for alarms monitored over data networks.

e. Alarm investigator response time exceeds 15 minutes.

5-905. Certification of Compliance. Evidence of compliance with the requirements of this section will consist of a valid (current) UL Certificate for the appropriate category of service. This certificate will have been issued to the protected facility by UL, through the alarm installing company. The certificate serves as evidence that the alarm installing company: (a) is listed as furnishing security systems of the category indicated; (b) is authorized to issue the certificate of installation as representation that the equipment is in compliance with requirements established by UL for the class; and (c) is subject to the UL field countercheck program whereby periodic inspections are made of representative alarm installations by UL personnel to verify the correctness of certification practices.

5-906. Exceptional Cases

a. If the requirements set forth above cannot be met, the contractor may request CSA approval for an alarm system meeting one of the conditions listed below. CSA approval will be documented on the Alarm System Description Form.

(1) Monitored by a central control station but responded to by a local (municipal, county, state) law enforcement organization.

(2) Connected by direct wire to alarm receiving equipment located in a local (municipal, county, state) police station or public emergency service dispatch center. This alarm system is activated and deactivated by employees of the contractor, but the alarm is monitored and responded to by personnel of the monitoring police or emergency service dispatch organization. Personnel monitoring alarm signals at police stations or dispatch centers do not require PCLs. Police department response systems may be requested only when: (a) the contractor facility is located in an area where central control station services are not available with line security and/or proprietary security force personnel, or a contractually-dispatched response to an alarm signal cannot be achieved within the time

limits required by the CSA, and, (b) it is impractical for the contractor to establish a GCMS or proprietary guard force at that location. Nonetheless, installation of these systems must use UL-listed equipment and be accomplished by an ASC Service Center listed by UL for any of the following categories:

1. Defense (National) Industrial Security Systems

2. Proprietary Alarm Systems

3. Central Station Burglar Alarm Systems

4. Police - Station - Connected Burglar Alarm Systems

b. An installation proposal, explaining how the system would operate, shall be submitted to the CSA. The proposal must include sufficient justification for the granting of an exception and the full name and address of the police department that will monitor the system and provide the required response. The name and address of the UL listed company that will install the system, and inspect, maintain, and repair the equipment, shall also be furnished.

c. The contractor shall require a 15-minute response time from the police department. Arrangements shall be made with the police to immediately notify a contractor representative on receipt of the alarm. The contractor representative is required to go immediately to the facility to investigate the alarm and to take appropriate measures to secure the classified material.

d. In exceptional cases where central station monitoring service is available, but no proprietary security force, central station, or subcontracted guard response is available, and where the police department does not agree to respond to alarms, and no other manner of investigative response is available, the CSA may approve cleared employees as the sole means of response.

CHAPTER 6
Visits and Meetings

Section 1. Visits

6-100. General. This section applies when, for a lawful and authorized U.S. Government purpose, it is anticipated that classified information will be disclosed during a visit to a cleared contractor or to a Federal facility.

6-101. Classified Visits. The number of classified visits shall be held to a minimum. The contractor must determine that the visit is necessary and that the purpose of the visit cannot be achieved without access to, or disclosure of, classified information. Contractors shall establish procedures to ensure positive identification of visitors, appropriate PCL, and need-to-know prior to the disclosure of any classified information. Contractors shall establish procedures to ensure that visitors are only afforded access to classified information consistent with the purpose of the visit.

6-102. Need-to-Know Determination. The responsibility for determining need-to-know in connection with a classified visit rests with the individual who will disclose classified information during the visit. Need-to-know is generally based on a contractual relationship between the contractors. In other circumstances, disclosure of the information will be based on an assessment that the receiving contractor has a bona fide need to access the information in furtherance of a GCA purpose.

6-103. Visits by Government Representatives. Representatives of the Federal Government, when acting in their official capacities as inspectors, investigators, or auditors, may visit a contractor's facility, provided these representatives present appropriate government credentials upon arrival.

6-104. Visit Authorization

a. If a visit requires access to classified information, the host contractor shall verify the visitor's PCL level. Verification of a visitor's PCL may be accomplished by a review of a CSA-designated database that contains the information or by a visit authorization letter (VAL) provided by the visitor's employer.

b. If a CSA-designated database is not available and a VAL is required, contractors shall include the following information in all VALs.

(1). Contractor's name, address, and telephone number, assigned Commercial and Government Entity (CAGE) code, if applicable, and certification of the level of the facility security clearance;

(2). Name, date and place of birth, and citizenship of the employee intending to visit;

(3). Certification of the proposed visitor's PCL and any special access authorizations required for the visit;

(4). Name of person(s) to be visited;

(5). Purpose and sufficient justification for the visit to allow for a determination of the necessity of the visit; and

(6). Date or period during which the VAL is to be valid.

6-105. Long-Term Visitors

a. When government employees or employees of one contractor are temporarily stationed at another contractor's facility, the security procedures of the host contractor will govern.

b. Government personnel assigned to or visiting a contractor facility and engaged in oversight of an acquisition program shall retain control of their work product. Classified work products of government employees shall be handled in accordance with this manual. Contractor procedures shall not require government employees to relinquish control of their work products, whether classified or not, to a contractor.

c. Contractor employees at government installations shall follow the security requirements of the host. However, this does not relieve the contractor from security oversight of their employees who are long-term visitors at government installations.

Section 2. Meetings

6-200. General. This section applies to a conference, seminar, symposium, exhibit, convention, training course, or other such gathering during which classified information is disclosed, hereafter called a "meeting."

6-201. Government Sponsorship of Meetings. Disclosure of classified information to large diverse audiences such as conferences increases security risks. However, classified disclosure at such meetings which serve a government purpose and at which adequate security measures have been provided in advance may be conducted by a cleared contractor provided the meeting is authorized by a government agency that has agreed to assume security jurisdiction. The government agency must approve security arrangements, announcements, attendees, and the location of the meeting. The government agency may delegate certain responsibilities to a cleared contractor for the security arrangements and other actions necessary for the meeting under the general supervision of the government agency.

a. **Requests for Authorization.** Contractors desiring to conduct meetings requiring sponsorship shall submit their requests to the Government Agency having principal interest in the subject matter of each meeting. The request for authorization shall include the following information:

(1) An explanation of the government purpose to be served by disclosing classified information at the meeting and why the use of conventional channels for release of the information will not advance those interests.

(2) The subject of the meeting and scope of classified topics, to include the classification level, to be disclosed at the meeting.

(3) The expected dates and location of the meeting.

(4) The general content of the proposed announcement and/or invitation to be sent to prospective attendees or participants.

(5) The identity of any other non-government organization involved and a full description of the type of support it will provide.

(6) A list of any foreign representatives (including their nationality, name, organizational affiliation) whose attendance at the meeting is proposed.

(7) A description of the security arrangements necessary for the meeting to comply with the requirements of this manual.

b. **Location of Meetings.** Classified sessions shall be held only at a Federal Government installation or a cleared contractor facility where adequate physical security and procedural controls have been approved. The authorizing government agency is responsible for evaluating and approving the location proposed for the meeting.

c. **Security Arrangements for Meetings.** The contractor shall develop the security measures and procedures to be used and obtain the authorizing agency's approval. The security arrangements must provide for the following:

(1) **Announcements.** Approval of the authorizing agency shall be obtained for all announcements of the meeting. Announcements shall be unclassified and shall be limited to a general description of topics expected to be presented, names of speakers, and administrative instructions for requesting invitations or participation. Classified presentations shall not be solicited in the announcement. When the meeting has been approved, announcements may only state that the government agency has authorized the conduct of classified sessions and will provide necessary security assistance. The announcement shall further specify that security clearances and justification to attend classified sessions are to be forwarded to the authorizing agency or its designee. Invitations to foreign persons shall be sent by the authorizing government agency.

(2) **Clearance and Need-to-know.** All persons in attendance at classified sessions shall possess the requisite clearance and need-to-know for the information to be disclosed. Need-to-know shall be determined by the authorizing agency or its designee based on the justification provided. Attendance shall be authorized only to those persons whose security clearance and justification for attendance have been verified by the security officer of the organization represented. The names of all authorized attendees or participants must appear on an access list with entry permitted to the classified session only after verification of the attendee's identity based

on presentation of official photographic identification such as a passport, contractor or U.S. Government identification card.

(3) **Presentations.** Classified information must be authorized for disclosure in advance by the government agency having jurisdiction over the information to be presented. Individuals making presentations at meetings shall provide sufficient classification guidance to enable attendees to identify what information is classified and the level of classification. Classified presentations shall be delivered orally and/or visually. Copies of classified presentations or slides, etc., shall not be distributed at the classified meeting, and any classified notes or electronic recordings of classified presentations shall be classified, safeguarded, and transmitted as required by this Manual.

(4) **Physical Security.** The physical security measures for the classified sessions shall provide for control of, access to, and dissemination of, the classified information to be presented and shall provide for secure storage capability, if necessary.

6-202. Disclosure Authority at Meetings. A contractor desiring to disclose classified information at a meeting shall:

a. Obtain prior written authorization for each proposed disclosure of classified information from the government agency having jurisdiction over the information involved.

b. Furnish a copy of the disclosure authorization to the government agency sponsoring the meeting.

c. Associations are not responsible for ensuring that classified presentations and papers of other organizations have been approved for disclosure. Authority to disclose classified information at meetings, whether disclosure is by officials of industry or government, must be granted by the government agency or activity that has classification jurisdiction over the information to be disclosed. Each contractor that desires to disclose classified information at a meeting is responsible for requesting and obtaining disclosure approvals.

6-203. Requests to Attend Classified Meetings. Before a contractor employee can attend a classified meeting, the contractor shall provide justification why the employee requires access to the classified information, cite the classified contract or GCA program/project involved, and forward the information to the authorizing government agency.

CHAPTER 7
Subcontracting

Section 1. Prime Contractor Responsibilities

7-100. General. This Chapter outlines the requirements and responsibilities of a prime contractor when disclosing classified information to a subcontractor.

7-101. Responsibilities. Before a prime contractor may release or disclose classified information to a subcontractor, or cause classified information to be generated by a subcontractor, the following actions are required:

a. Determine the security requirements of the subcontract.

(1) Access to classified information will be required. This is a "classified contract" within the meaning of this Manual. A "security requirements clause" and a Contract Security Classification Specification shall be incorporated in the solicitation and in the subcontract (see the "security requirements clause" in the prime contract). The subcontractor must possess an appropriate FCL and safeguarding capability if possession of classified information will be required.

(a) If access will not be required in the pre-award phase, prospective subcontractors are not required to possess an FCL to receive or bid on the solicitation.

(b) If access will be required during the pre-award phase, all prospective subcontractors must possess the appropriate FCL and have safeguarding capability.

(2) Access to classified information will not be required. This is not a classified contract within the meaning of this Manual. If the prime contract contains requirements for release or disclosure of certain information even though not classified, such as sensitive but unclassified information, the requirements shall be incorporated in the solicitation and the subcontract.

b. Determine clearance status of prospective subcontractors.

(1) All prospective subcontractors have appropriate clearance. This determination can be made if there is an existing contractual relationship between the parties involving classified information of the same or higher category, by accessing the CSA-designated database, or by contacting the CSA.

(2) If a prospective subcontractor does not have the appropriate FCL or safeguarding capability, the prime contractor shall request the CSA of the subcontractor to initiate the necessary action. Requests shall include, as a minimum, the full name, address and contact information for the requester; the full name, address, and contact information for a contact at the facility to be processed for an FCL; the level of clearance and/or safeguarding capability required; and full justification for the request. Requests for safeguarding capability shall include a description, quantity, end-item, and classification of the information related to the proposed subcontract. Other factors necessary to help the CSA determine if the prospective subcontractor meets the requirements of this manual shall be identified, such as any special access requirements.

c. Requesting contractors shall allow sufficient lead time in connection with the award of a classified subcontract to enable an uncleared bidder to be processed for the necessary FCL. When the FCL cannot be granted in sufficient time to qualify the prospective subcontractor for participation in the current procurement action, the CSA will continue the FCL processing action to qualify the prospective subcontractor for future contract consideration provided:

(1) The delay in processing the FCL was not caused by a lack of cooperation on the part of the prospective subcontractor;

(2) Future classified negotiations may occur within 12 months; and

(3) There is reasonable likelihood the subcontractor may be awarded a classified subcontract.

7-102. Security Classification Guidance. Prime contractors shall ensure that a Contract Security Classification Specification is incorporated in each classified subcontract. When preparing classification

guidance for a subcontract, the prime contractor may extract pertinent information from the Contract Security Classification Specification issued with the prime contract; from security classification guides issued with the prime contract; or from any security guides that provide guidance for the classified information furnished to, or that will be generated by, the subcontractor. The Contract Security Classification Specification prepared by the prime contractor shall be certified by a designated official of the contractor. In the absence of exceptional circumstances, the classification specification shall not contain any classified information. If classified supplements are required as part of the Contract Security Classification Specification, they shall be identified and forwarded to the subcontractor by separate correspondence.

a. An original Contract Security Classification Specification shall be included with each RFQ, RFP, IFB, or other solicitation to ensure that the prospective subcontractor is aware of the security requirements of the subcontract and can plan accordingly. An original Contract Security Classification Specification shall also be included in the subcontract awarded to the successful bidder.

b. A revised Contract Security Classification Specification shall be issued as necessary during the lifetime of the subcontract when the security requirements change.

c. Requests for public release by a subcontractor shall be forwarded through the prime contractor to the GCA.

7-103. Responsibilities (Completion of the Subcontract). Upon completion of the subcontract, the subcontractor may retain classified material received or generated under the subcontract for a 2-year period, provided the prime contractor or GCA does not advise to the contrary. If retention is required beyond the 2-year period, the subcontractor must request written retention authority through the prime contractor to the GCA. If retention authority is approved by the GCA, the prime contractor will issue a final Contract Security Classification Specification, annotated to provide the retention period and final disposition instructions.

7-104. Notification of Unsatisfactory Conditions. The prime contractor shall be notified if the CSA discovers unsatisfactory security conditions in a subcontractor's facility. When so notified, the prime contractor shall follow the instructions received relative to what action, if any, should be taken in order to safeguard classified material relating to the subcontract.

CHAPTER 8
Information System Security

Section 1. Responsibilities and Duties

8-100. General

a. Information systems (IS) that are use-d to capture, create, store, process or distribute classified information must be properly managed to protect against unauthorized disclosure of classified information, loss of data integrity to ensure the availability of the data and system.

b. Protection requires a balanced approach including IS security features to include but not limited to, administrative, operational, physical, computer, communications, and personnel controls. Protective measures commensurate with the classification of the information, the threat, and the operational requirements associated with the environment of the IS are required.

c. The requirements outlined in the following sections apply to all information systems processing classified information. Additional requirements for high-risk systems and data are covered in the NISPOM Supplement

8-101. Responsibilities

a. The CSA shall establish a line of authority for training, oversight, program review, certification, and accreditation of IS used by contractors for the processing of classified information. The CSA will conduct a risk management evaluation based on the contractor's facility, the classification, and sensitivity of the information processed. The evaluation must ensure that a balanced, cost-effective application of security disciplines and technologies is developed and maintained.

b. Contractor management will publish and promulgate an IS Security Policy addressing the classified processing environment. Additionally, an IS Security Manager (ISSM) will be appointed with oversight responsibility for the development, implementation, and evaluation of the facility's IS security program. Contractor management will assure that the ISSM is trained to a level commensurate with the complexity of the facility's IS.

8-102. Designated Accrediting/Approving Authority. The CSA is the Designated Accrediting/Approving Authority (DAA) responsible for accrediting information systems used to process classified information in industry

8-103. IS Security Manager (ISSM). The ISSM:

a. Ensures the development, documentation, and presentation of IS security education, awareness, and training activities for facility management, IS personnel, users, and others, as appropriate.

b. Establishes, documents, implements, and monitors the IS Security Program and related procedures for the facility and ensures facility compliance with requirements for IS.

c. Identifies and documents unique local threats/vulnerabilities to IS.

d. Coordinates the facility IS Security Program with other facility security programs.

e. Ensures that periodic self-inspections of the facility's IS Program are conducted as part of the overall facility self-inspection program and that corrective action is taken for all identified findings and vulnerabilities. Self-inspections are to ensure that the IS is operating as accredited and that accreditation conditions have not changed.

f. Ensures the development of facility procedures to:

(1) Govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information.

(2) Properly implement vendor supplied authentication (password, account names) features or security-relevant features.

(3) Report IS security incidents to the CSA. Ensure proper protection or corrective measures have

been taken when an incident/vulnerability has been discovered.

(4) Require that each IS user sign an acknowledgment of responsibility for the security of the IS.

(5) Implement security features for the detection of malicious code, viruses, and intruders (hackers), as appropriate.

g. Certifies to the CSA, in writing, that each System Security Plan (SSP) has been implemented; that the specified security controls are in place and properly tested; and that the IS is functioning as described in the SSP.

h. Ensures notification of the CSA when an IS no longer processes classified information, or when changes occur that might affect accreditation.

i. Ensures that personnel are trained on the IS's prescribed security restrictions and safeguards before they are initially allowed to access a system.

j. Develops and implements general and remote maintenance procedures based on requirements provided by the CSA.

8-104. Information System Security Officer(s) (ISSO). ISSOs may be appointed by the ISSM in facilities with multiple accredited IS. The ISSM will determine the responsibilities to be assigned to the ISSO that may include the following:

a. Ensure the implementation of security measures, in accordance with facility procedures.

b. Identify and document any unique threats.

c. If so directed by the GCA and/or if an identified unique local threat exists, perform a risk assessment to determine if additional countermeasures beyond those identified in this chapter are required.

d. Develop and implement a certification test as required by the ISSM/CSA.

e. Prepare, maintain, and implement an SSP that accurately reflects the installation and security provisions.

f. Notify the CSA (through the ISSM) when an IS no longer processes classified information, or when changes occur that might affect accreditation.

g. Ensure:

(1) That each IS is covered by the facility Configuration Management Program, as applicable.

(2) That the sensitivity level of the information is determined prior to use on the IS and that the proper security measures are implemented to protect this information.

(3) That unauthorized personnel are not granted use of, or access to, an IS.

(4) That system recovery processes are monitored to ensure that security features and procedures are properly restored.

h. Document any special security requirement identified by the GCA and the protection measures implemented to fulfill these requirements for the information contained in the IS.

i. Implement facility procedures:

(1) To govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information.

(2) To ensure that vendor-supplied authentication (password, account names) features or security-relevant features are properly implemented.

(3) For the reporting of IS security incidents and initiating, with the approval of the ISSM, protective or corrective measures when a security incident or vulnerability is discovered.

(4) Requiring that each IS user sign an acknowledgment of responsibility for the security of IS and classified information.

(5) For implementing and maintaining security-related software for the detection of malicious code, viruses, and intruders (hackers), as appropriate.

j. Conduct ongoing security reviews and tests of the IS to periodically verify that security features and operating controls are functional and effective.

k. Evaluate proposed changes or additions to the IS, and advises the ISSM of their security relevance.

l. Ensure that all active user Ids are revalidated at least annually.

8-105. Users of IS. Users of IS are either privileged or general users.

a. Privileged users have access to IS control, monitoring or administration functions. Examples include:

(1) Users having "superuser," "root," or equivalent access to a system (e.g., system administrators, computer operators, ISSOs); users with near or complete control of an IS or who set up and administer user accounts and authenticators.

(2) Users having access to change control parameters (routing tables, path priorities, addresses, etc.) on routers, multiplexers, and other key IS equipment.

(3) Users who have been given the authority to control and change other users' access to data or program files (e.g., applications software administrators, administrators of specialty file systems, database managers).

(4) Users who have been given special access for troubleshooting or monitoring an IS' security functions (e.g., those using analyzers, management tools).

b. General users are individuals who can input information to or modify information on an IS or who can receive information from an IS without a reliable human review.

c. All users shall:

(1) Comply with the IS Security Program requirements.

(2) Be aware of and knowledgeable about their responsibilities in regard to IS security.

(3) Be accountable for their actions on an IS.

(4) Ensure that any authentication mechanisms (including passwords) issued for the control of their access to an IS are not shared and are protected at the highest classification level and most restrictive classification category of information to which they permit access.

(5) Acknowledge, in writing, their responsibilities for the protection of the IS and classified information.

Section 2. Certification and Accreditation

8-200. Overview. The certification and accreditation (C&A) process is an integral part of the life cycle of an IS. The identification of protection measures occurs during system design or development. The formal C&A occurs after the protection measures have been implemented and any required IS protection documentation has been approved. Certification validates that the protection measures described in the SSP have been implemented on the system and that the protection measures are functioning properly. Accreditation is the approval by the CSA for the system to process classified information.

8-201. Certification Process. Certification is the comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made as part of and in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements. The certification process subjects the system to appropriate verification that protection measures have been correctly implemented. The ISSM shall review and certify to the CSA that all systems have the appropriate protection measures in place and validate that they provide the protection intended. The CSA may conduct an on site assessment to validate the ISSM's review and certification of the IS.

8-202. Accreditation. The accreditation of an IS is the official management decision to permit operation of an IS in a specified environment at an acceptable level of risk, based on the implementation of a CSA approved set of technical, managerial and procedural safeguards. All IS certifications shall be reviewed and IS accredited to operate by the CSA.

a. **Interim Approval to Operate.** The CSA may grant interim approval (temporary authority) to operate an IS. Interim approval to operate may be granted for up to 180 days with an option for the CSA to extend the interim approval for an additional 180 days. CSA-approved protection measures shall be in place and functioning during the period of interim approval.

b. **Reaccreditation.** IS shall be reaccredited whenever security relevant changes are made to the accredited IS. Proposed modifications to an IS shall be reviewed by the ISSM to determine if the proposed modifications will impact the protections on the system. If the protection aspects of the system's environment change, if the applicable IS protection requirements change, or if the protection mechanisms implemented for the system change, the system shall be reaccredited. During the reaccreditation cycle, the CSA may grant an interim approval to operate the system.

c. **Review of Security-Relevant Changes.** All modifications to security-relevant resources (including software, firmware, hardware, or interfaces and interconnections to networks) shall be reviewed and approved in accordance with procedures prior to implementation. All security-relevant changes shall be subject to the provisions of the system configuration management program. The ISSM shall notify the CSA of requests for changes to the resources that deviate from the requirements of the approved SSP. The CSA shall determine if system reaccreditation is required.

d. **Re-evaluation of an Accreditation.** Each IS shall be re-evaluated for reaccreditation every 3 years. Such review involves a determination by the CSA, with input from the ISSM that the conditions under which the original accreditation was granted still apply. If the accreditation remains valid, the accreditation originally furnished by the CSA need only be annotated that the re-evaluation was conducted and the date of the re-evaluation.

e. **Withdrawal of Accreditation.** The CSA shall evaluate the risks and consider withdrawal of accreditation if the protection measures approved for the system do not remain effective or whenever any of the following items change: levels of concern, protection level, technical or nontechnical protection measures, vulnerabilities, operational environment, operational concept, or interconnections. The CSA shall withdraw accreditation and ensure proper sanitization when the system is no longer required to process classified information, or if the operational need for the system no longer outweighs the risk of operating the system.

f. **Invalidation of an Accreditation.** The CSA will be notified and an accreditation will become invalid immediately whenever detrimental, security-significant changes occur to any of the following: the required protection level; the operational environment; or the interconnections.

g. **Certification and Accreditation of Similar Systems.** If two or more similar IS are to be operated

in equivalent operational environments (e.g., the levels of concern and protection level are the same, the users have at least the required clearances and access approvals for all information on the IS, the IS configurations are essentially the same, and the physical security requirements are similar), a Master SSP may be written by the ISSO, certified by the ISSM, and then approved by the CSA to cover all such IS. The IS covered by a Master SSP may range from stand alone workstations up to and including multi-user IS and local networks that meet the criteria for a Master SSP approach. This type of approval applies only to systems operating at Protection Levels 1 and 2 (see 8-402).

(1) Master Information Systems Security Plan. The Master SSP shall specify the information required for each certification for an IS to be accredited under the plan.

(2) An IS Certification Report shall contain the information system identification and location and a statement signed by the ISSM certifying that the IS implements the requirements in the Master SSP.

(3) The CSA shall accredit the first IS under the Master SSP. All other IS to be operated under the Master SSP shall be certified by the ISSM as meeting the conditions of the approved Master SSP. This certification, in effect, accredits the individual IS to operate under the Master SSP. A copy of each certification report shall be retained with the approved copy of the Master SSP.

(4) Recertification. IS certified under a Master SSP remain certified until the Master SSP is changed or 3 years have elapsed since the IS was certified. If either the levels of concern or protection level described in the Master SSP change, the Master SSP shall be re-accredited by the CSA and all IS certified under the Master SSP shall be re-certified by the ISSM in coordination with the CSA.

h. **Systems under Multiple CSAs.** For a system that involves multiple CSAs, the CSAs shall designate a primary CSA. Each facility involved in the system shall identify, in writing, the security officials who are responsible for implementing IS protection on the system components at their respective facility.

Section 3. Common Requirements

8-300. Introduction. This section describes the protection requirements that are common to all IS.

8-301. Clearing and Sanitization. Instructions on clearing, sanitization and release of IS media shall be issued by the accrediting CSA.

a. **Clearing.** Clearing is the process of eradicating the data on media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing. All internal memory, buffer, or other reusable memory shall be cleared to effectively deny access to previously stored information.

b. **Sanitization.** Sanitization is the process of removing the data from media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was in the media before sanitizing. IS resources shall be sanitized before they are released from classified information controls or released for use at a lower classification level.

8-302. Examination of Hardware and Software. IS hardware and software shall be examined when received from the vendor and before being placed into use.

a. **IS Software.** Commercially procured software shall be tested to ensure that the software contains no obvious features that might be detrimental to the security of the IS. Security-related software shall be tested to verify that the security features function as specified.

b. **IS Hardware.** Hardware shall be examined to determine that it appears to be in good working order and has no elements that might be detrimental to the secure operation of the IS when placed under facility control and cognizance. Subsequent changes and developments that affect security may require additional examination.

8-303. Identification and Authentication Management. As the complexity of a specific IS and the associated residual risk for this system increase, the need for identification and authentication of users and process becomes more significant. Identification and authentication controls are required to ensure that users have the appropriate clearances and need-to-know for the information on a particular system and shall be managed in accordance with procedures identified in the SSP.

a. **Unique Identification.** Each user shall be uniquely identified and that identity shall be associated with all auditable actions taken by that individual.

b. **Authentication at Logon.** Users shall be required to authenticate their identities at "logon" time by supplying their authenticator, such as a password, smart card, or biometrics, in conjunction with their user identification (ID) prior to the execution of any application or utility on the system.

c. **Applicability of Logon Authentication.** In some cases, it may not be necessary to use IS security controls as logon authenticators. In the case of stand alone workstations, or small local area networks, physical security controls and personnel security controls may suffice. For example, if the following conditions are met, it may not be necessary for the IS to have a logon and password:

(1) The workstation does not have a permanent (internal) hard drive, and the removable hard drive and other associated storage media are stored in an approved security container when not in use.

(2) All of the users with access to the workstation and the security container/ removable media have the required clearance level and need-to-know for all of the data processed on the workstation.

(3) The workstation is located within an approved security area, and all uncleared/lower-cleared personnel are escorted within the area.

d. **Access to Authentication Data.** Access to authentication data shall be restricted to authorized personnel through the use of encryption or file access controls, or both.

e. **User ID Reuse.** Prior to reuse of a user ID, all previous access authorizations (including file

accesses for that user ID) shall be removed from the system.

f. **User ID Removal.** When an employee terminates, loses access to the system for cause, or no longer has a reason to access the IS, that individual's user ID and its authentication shall be disabled or removed from the system.

g. **User ID Revalidation.** Active user IDs are revalidated at least annually.

h. **Protection of Individual Authenticator.** An authenticator that is in the form of knowledge (password) or possession (smart card, keys) shall not be shared with anyone.

i. **Protection of Individual Passwords.** When passwords are used as authenticators, the following shall apply:

(1) Passwords shall be protected at a level commensurate with the sensitivity level or classification level and classification category of the information to which they allow access.

(2) Passwords shall contain a minimum of eight non-blank characters, shall be valid for no longer than 12 months and changed when compromised.

(3) Passwords shall be generated by a method approved by the CSA. Password acceptability shall be based on the method of generation, the length of the password, password structure, and the size of the password space. The password generation method, the length of the password, and the size of the password space shall be described in an attachment to the SSP.

(4) When an IS cannot prevent a password from being echoed (e.g., in a half-duplex connection), an overprint mask shall be printed before the password is entered to conceal the typed password.

(5) User software, including operating system and other security-relevant software, comes with a few standard authenticators (e.g., SYSTEM, TEST, and MASTER) and passwords already enrolled in the system. The ISSO shall ensure that the passwords for all standard authenticators are changed before allowing the general user population access to the IS. The ISSO shall also ensure that these passwords are changed after a new system version is installed or after other action is taken that might result in the restoration of these standard passwords.

8-304. Maintenance. IS are particularly vulnerable to security threats during maintenance activities. The level of risk is a factor of the nature of the maintenance person's duties, the security awareness of the employees, and the maintenance person's access to classified information and facilities.

a. **Cleared Maintenance Personnel.** Maintenance personnel who are cleared to the highest classification level of information on the system and indoctrinated for all information processed on that system do not require an escort, if need-to-know controls can be implemented. When possible, an appropriately cleared and technically knowledgeable, facility employee shall be present within the area where the maintenance is being performed to ensure that security procedures are being followed.

b. **Uncleared (or Lower-Cleared) Maintenance Personnel**

(1) If appropriately cleared personnel are unavailable to perform maintenance, an uncleared or lower-cleared person may be used, provided an appropriately cleared and technically qualified escort monitors and records the maintenance person's activities in a maintenance log. Uncleared maintenance personnel must be U.S. citizens.

(2) System initiation and termination shall be performed by the escort. In addition, keystroke monitoring shall be performed during access to the system.

(3) Prior to maintenance, the IS shall be completely cleared and all non-volatile data storage media shall be removed or physically disconnected and secured. When a system cannot be cleared procedures, which are identified in the SSP, shall be enforced to deny the maintenance personnel visual and electronic access to any classified data contained on the system.

(4) A separate, unclassified copy of the operating system, including any micro-coded floppy disks, CD-ROM, or cassettes that are integral to the operating system, shall be used for all maintenance operations. The copy shall be labeled "UNCLASSIFIED -- FOR MAINTENANCE ONLY" and protected in accordance with procedures established in the SSP. Maintenance procedures for an IS using a non-removable storage device on which the operating system is resident shall be considered by the ISSM on a case-by-case basis.

8-305. Malicious Code. Policies and procedures to detect and deter incidents caused by malicious code, such as viruses or unauthorized modification to software, shall be implemented. All files must be checked for viruses before being introduced on an IS and checked for other malicious code as feasible. The use of personal or public domain software is strongly discouraged. Each installation of such software must be approved by the ISSM.

8-306. Marking Hardware, Output, and Media. Markings on hardware, output, and media shall conform to Chapter 4 of this manual. If the required marking is impractical or interferes with the operation of the media, the CSA may approve alternate marking procedures.

a. **Hardware Components.** All components of an IS, including input/output devices that have the potential for retaining information, terminals, stand-alone microprocessors, or word processors used as terminals, shall bear a conspicuous, external label that states the highest classification level and most restrictive classification category of the information accessible to the component in the IS. This labeling may be accomplished using permanent markings on the component, a sign placed on the terminal, or labels generated by the IS and displayed on the screen. If the CSA requires that labels be color coded to indicate classification level they shall be orange for Top Secret, red for Secret, blue for Confidential, and green for unclassified.

b. **Hard Copy Output and Removable Media.** Hard copy output (paper, fiche, film, and other printed media) and removable media shall be marked with visible, human-readable, external markings to the accreditation level of the IS unless an appropriate classification review has been conducted or in the case of media, the information has been generated by a tested program verified to produce consistent results and approved by the CSA. Such programs will be tested on a statistical basis to ensure continuing performance.

c. **Unclassified Media.** In the CSA-approved areas where classified and unclassified information are processed on collocated IS, unclassified media shall be so marked.

8-307. Personnel Security. Personnel with system access play an integral role in protecting information; defining their system security policies; and maintaining and monitoring the confidentiality, integrity, and availability attributes that are inherent within their IS. Duties, responsibilities, privileges, and specific limitations of IS users, both general and privileged, shall be specified in writing. So far as feasible, security duties shall be distributed to preclude any one individual from adversely affecting operations or the integrity of the system. Protection levels for particular IS shall be determined by the clearance level, formal access approvals, and need-to-know held by users of the IS, and the classification level of data processed or stored.

8-308. Physical Security

a. Safeguards shall be established that prevent or detect unauthorized access to the IS and unauthorized modification of the IS hardware and software. Hardware integrity of the IS, including remote equipment, shall be maintained at all times, even when all classified information has been removed from the IS.

b. Classified processing shall take place in a CSA-approved area.

c. Visual Access. Devices that display or output information in human-readable form shall be positioned to prevent unauthorized individuals from reading the information.

d. Unescorted Access. All personnel granted unescorted access to the area containing the IS shall have an appropriate security clearance.

8-309. Protection of Media. Media must be protected to the level of accreditation until an appropriate classification review has been conducted.

8-310. Review of Output and Media

a. **Human-Readable Output Review.** An appropriate sensitivity and classification review shall be performed on human-readable output before the output is released outside the security boundary to determine whether it is accurately marked with the appropriate classification and applicable associated security markings.

b. **Media Review.** Electronic output, such as files, to be released outside the security boundary shall be verified by a comprehensive review (in human-readable form) of all data on the media including embedded text (e.g., headers and footer) before being released. Information on media that is not in human-readable form (e.g., embedded graphs, sound, video, etc.) will be examined for content using the appropriate software application. CSA-approved random or representative sampling techniques may

be used to verify the proper marking of large volumes of output.

8-311. Configuration Management. Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system.

a. **Configuration Documentation.** Procedures shall be implemented to identify and document the type, model, and brand of system or network component (e.g., a workstation, personal computer, or router), security-relevant software product names and version or release numbers, and physical location.

b. **System Connectivity.** Procedures shall be implemented to identify and document system connectivity, including any software used for wireless communication, and any communications media.

c. **Connection Sensitivity.** The sensitivity level of each connection or port controlled by the Security Support Structure (SSS) shall be documented.

d. **CM Plan.** The facility CM program shall be documented in a CM plan and shall include:

(1) Formal change control procedures to ensure the review and approval of security-relevant hardware and software.

(2) Procedures for management of all documentation, such as the SSP and security test plans, used to ensure system security.

(3) Workable processes to implement, periodically test, and verify the CM plan.

(4) A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted.

Section 4. Protection Measures

8-400. Protection Profiles. Protection profiles required for a particular IS are determined by the Level of Concern for Confidentiality and by the operating environment of the system as reflected by the clearances, access approvals and need-to-know embodied in the user environment. Operational data integrity and system availability, while important security concerns, are not covered by the NISP and will be determined in additional guidance or requirements issued by the GCA. However, provisions for integrity and availability concerns are included in this Chapter to provide guidance when the GCA contractually imposes them.

8-401. Level of Concern. The level of concern reflects the sensitivity of the information and the consequences of the loss of confidentiality, integrity or availability.

a. **Information Sensitivity Matrices.** The matrices presented in Tables 1, 2, and 3 are designed to assist the CSA, with input from the ISSM in determining the appropriate protection level for confidentiality, and the level of concern for integrity, and availability, if contractually mandated, for a given IS processing a given set of information. The Information Sensitivity Matrices should be used as follows:

(1) A determination of high, medium, or basic shall be made for each of the three attributes: confidentiality, integrity, and availability. It is not necessary for the level of concern to be the same for all attributes of the system.

(2) When multiple applications on a system result in different levels of concern for the categories of confidentiality, integrity and availability the highest level of concern for each category shall be used.

b. **Confidentiality Level of Concern.** In considering confidentiality, the principal question is the necessity for supporting the classification levels and the categories of information (e.g., Secret National Security Information) on the system in question. The Protection Level Table for Confidentiality (Table 4) combines the processing environment with the level of concern for confidentiality to provide a Protection Level. The Protection Level is then applied to Table 5 to provide a set of graded requirements to protect the confidentiality of the information on the system.

c. **Integrity Level of Concern.** In considering integrity, the principal question is the necessity for maintaining the integrity of the information on the system in question.

d. **Availability Level of Concern.** In considering availability, the principal consideration is the need for the information on the system in question to be available in a fixed time frame to accomplish a mission.

8-402. Protection Level. The protection level of an IS is determined by the relationship between two parameters: first, the clearance levels, formal access approvals, and need-to-know of users; and second, the level of concern based on the classification of the data on a particular system. The protection level translates into a set of requirements (tables 5, 6, and 7) that must be implemented in the resulting system. Table 4 presents the criteria for determining the following three protection levels for confidentiality.

a. Systems are operating at Protection Level 1 when all users have all required approvals for access to all information on the system. This means that all users have all required clearances, formal access approvals, and the need-to-know for all information on the IS, i.e. dedicated mode.

b. Systems are operating at Protection Level 2 when all users have all required clearances, and all required formal access approvals, but at least one user lacks the need-to-know for some of the information on the system, i.e. a system high mode.

c. Systems are operating at Protection Level 3 when all users have all required clearances, but at least one user lacks formal access approval for some of the information on the system, i.e. compartmented mode.

8-403. Protection Profiles. Protection requirements graded by levels of concern and confidentiality protection level are detailed in Section 6. Tables 5, 6, and 7 present the requirements detailed in Section 6. To use these tables, find the column representing the protection level for confidentiality, or, if contractually mandated, find the column representing the level of concern for integrity or availability.

a. **Confidentiality Components.** Confidentiality components describe the confidentiality protection requirements that must be implemented in an IS using the profile. The confidentiality protection requirements are graded according to the confidentiality protection levels.

b. **Integrity Components.** Integrity components, if applicable, describe the integrity protection requirements that must be implemented in an IS using the profile. The integrity protection requirements are graded according to the integrity level of concern.

c. **Availability Components.** Availability components, if applicable, describe the availability protection requirements that must be implemented in an IS using the profile. The availability protection requirements are graded according to the availability level of concern**.**

Table 1. Information Sensitivity Matrix for Confidentiality

Level of Concern	Qualifiers
High	TOP SECRET and SECRET Restricted Data (SIGMAs 1,2,14,15)
Medium	SECRET SECRET Restricted Data
Basic	CONFIDENTIAL

Table 2. Information Sensitivity Matrix for Integrity

Level of Concern	Qualifiers
High	Absolute accuracy required for mission accomplishment; or loss of life might result from loss of integrity; or loss of integrity will have an adverse effect on national-level interests; or loss of integrity will have an adverse effect on confidentiality.
Medium	High degree of accuracy required for mission accomplishment, but not absolute; or bodily injury might result from loss of integrity; or loss of integrity will have an adverse effect on organizational-level interests.
Basic	Reasonable degree of accuracy required for mission accomplishment.

Table 3. Information Sensitivity Matrix for Availability

Level of Concern	Qualifiers
High	Information must always be available upon request, with no tolerance for delay; or loss of life might result from loss of availability; or loss of availability will have an adverse effect on national-level interests; or loss of availability will have an adverse effect on confidentiality.
Medium	Information must be readily available with minimum tolerance for delay; or bodily injury might result from loss of availability; or loss of availability will have an adverse effect on organizational-level interests.
Basic	Information must be available with flexible tolerance for delay.

NOTE: In this context, “High - no tolerance for delay” means no delay; “Medium - minimum tolerance for delay” means a delay of seconds to hours; and “Basic - flexible tolerance for delay” means a delay of days to weeks. In the context of the NISPOM, integrity and availability shall only apply when the have a direct impact on protection measures for confidentiality, i.e., integrity of the password file, integrity of audit logs or when contractually imposed.

Table 4. Protection Level Table for Confidentiality

Level of Concern	Lowest Clearance	Formal Access Approval	Need-To-Know	Protection Level
High, Medium, or Basic	At Least Equal to Highest Data	NOT ALL Users Have ALL	Not contributing to the decision	3
High, Medium, or Basic	At Least Equal to Highest Data	ALL Users Have ALL	NOT ALL Users Have ALL	2
High, Medium, or Basic	At Least Equal to Highest Data	ALL Users Have ALL	ALL Users Have ALL	1

Table 5. Protection Profile Table for Confidentiality

	Confidentiality Protection Level		
Requirements (Paragraph)	P L 1	PL 2	PL 3
Audit Capability (8-602)	Audit 1	Audit 2	Audit 3 Audit 4
Data Transmission (8-605)	Trans 1	Trans 1	Trans 1
Access Controls (8-606)	Access 1	Access 2	Access 3
Identification & Authentication (8-607)	I&A 1	I&A 2,3,4	I&A2,4,5
Resource Control (8-608)		ResrcCtrl 1	ResrcCtrl 1
Session Controls (8-609)	SessCtrl 1	SessCtrl 2	SessCtrl 2
Security Documentation (8-610)	Doc 1	Doc 1	Doc 1
Separation of Functions (8-611)			Separation
System Recovery (8-612)	SR 1	SR 1	SR 1
System Assurance (8-613)	SysAssur 1	SysAssur 1	SysAssur 2
Security Testing (8-614)	Test 1	Test 2	Test 3

Table 6. Protection Profile Table for Integrity

	Integrity Level of Concern		
Requirements (Paragraph)	Basic	Medium	High
Audit Capability (8-602)	Audit 1	Audit 2	Audit 3
Backup and Restoration of Data (8-603)	Backup 1	Backup 2	Backup 3
Changes to Data (8-604)		Integrity 1	Integrity 2
System Assurance (8-613)		SysAssur 1	SysAssur 2
Security Testing (8-614)	Test 1	Test 2	Test 3

Table 7. Protection Profile Table for Availability

	Availability Level of Concern		
Requirements (Paragraph)	Basic	Medium	High
Alternate Power Source (8-601)		Power 1	Power 2
Backup and Restoration of Data (8-603)	Backup 1	Backup 2	Backup 3

Section 5. Special Categories

8-500. Special Categories. Several categories of systems can be adequately secured without implementation of all the technical features specified this Chapter. These systems are not "exceptions" or "special cases" but applying the technical security requirements to these systems by rote results in unnecessary costs and operational impacts. In general, the technical questions are where, when, and how to apply a given set of protection measures, rather than whether to apply the measures. For many of these "special" systems (such as guards or pure servers; and tactical, embedded, data-acquisition, and special-purpose systems), the physical security protections for the system provide the required access control, while the application running on the platform provides the required user separation.

8-501. Single-user, Stand-alone Systems. Extensive technical protection measures are normally inappropriate and inordinately expensive for single-user, stand-alone systems. The CSA can approve administrative and environmental protection measures for such systems, in lieu of technical ones. Systems that have one user at a time, but have a total of more than one user with no sanitization between users, are multi-user systems, and the CSA shall consider the systems as such in determining the protection level and the resulting security requirements. Systems that have one user at a time, are sanitized between users and periods of different classification/sensitivity, are periods processing systems as described below.

8-502. Periods Processing. Periods processing is a method of sequential operation of an IS that provides the capability to process information at various levels of sensitivity at distinctly different times.

a. Periods processing provides the capability to either have more than one user or group of users (sequentially) on a single-user IS who do not have the same need-to-know or who are authorized to access different levels of information; or use an IS at more than one protection level (sequentially).

b. Sanitization After Use. If an IS is used for periods processing either by more than one user or for segregating information by classification level onto separate media, the SSP shall specify the sanitization procedures to be employed by each user before and after each use of the system.

c. Sanitization Between Periods. The IS shall be sanitized of all information before transitioning from one period to the next (e.g., whenever there will be a new user(s) who does not have an access authorization or need-to-know for data processed during the previous period, changing from one protection level to another). These procedures shall be documented in the SSP. Such procedures could include, among others, sanitizing non-volatile storage, exchanging disks, and powering down the IS and its peripherals.

d. Media For Each Period. An IS employed in periods processing shall have separate media for each period of processing, including copies of operating systems, utilities, and applications software.

e. Audit. If there are multiple users of the system and the system is not capable of automated logging, the CSA shall consider requiring manual logging. Audit trails are not required for single-user stand-alone systems.

8-503. Pure Servers

a. Certain specialized systems, when acting as pure servers in a network, do not fit the protection level criteria and may need fewer technical security countermeasures. These systems have the following characteristics:

(1) No user code is present on the system.

(2) Only system administrators and maintainers can access the system.

(3) The system provides non-interactive services to clients (e.g., packet routing or messaging services).

(4) The hardware and/or application providing network services otherwise meet the security requirements of the network.

(5) The risk of attack against the Security Support Structure (SSS) using network communication paths is sufficiently low.

(6) The risk of attack against the SSS using physical access to the system itself is sufficiently low.

b. The platform (i.e., hardware and operating system) on which the guard or pure server runs usually needs to meet no more than Protection Level 3 security requirements. The guard or pure server may have a large number of clients (i.e., individuals who use the guard or server functional capabilities in a severely constrained way). The guard application or server application itself will have to provide the more stringent technical protections appropriate for the system's protection level and operational environment. Assurances appropriate to the levels of concern for the system shall be implemented.

c. Systems that have general users or execute general user code are not "pure servers" within the meaning of this section, and so must meet all security requirements specified for their protection level and operational environment.

d. The term "pure server" is not intended to limit the applicability of this section to systems that have traditionally been referred to as servers. For example, a messaging system that happened to be implemented on a general-purpose computer platform could be accredited under this section and, if such a system meets the specifications in a, above, the system's technical requirements could be categorized by this section.

e. The above easing of technical security requirements does not imply any relaxation in other security requirements (e.g., physical and communications security requirements) which are determined by the information handled or protected by the system. As stated above, this easing of technical requirements is predicated upon adequate application of physical security and other appropriate security disciplines.

8-504. Tactical, Embedded, Data-Acquisition, and Special-Purpose Systems. Some systems are incapable of alteration by users and are designed and implemented to provide a very limited set of predetermined functions. Certain tactical or so-called "embedded" systems fall into this category, as do some data-acquisition systems and some other special-purpose systems. These systems also have the characteristics that: first and most importantly, there are no general users on the system; and, second, there is no user code running on the system. If the CSA determines that such a system is sufficiently incapable of alteration, and that the application(s) running on the system provide an adequate level of security, then the system does not have to meet additional security requirements specified for more-general-purpose systems in this section. The CSA and implementers are cautioned to be sure that such systems do, in all operational situations, provide the separation appropriate to the system's protection level.

8-505. Systems with Group Authenticators. Many security measures specified in this section implicitly assume that the system includes an acceptable level of individual accountability. This is normally ensured by the use of unique user identifiers and authenticators. Operationally, the design of some systems necessitates more than one individual using the same identifier/ authenticator combination. Such situations are often referred to as requiring the use of group authenticators. In general, the use of group authenticators precludes the association of a particular act with the individual who initiated that act. In turn, this can preclude assignment of responsibility and can exacerbate the difficulties involved in incident investigation. Group authenticators shall be used only for broader access after the use of a unique authenticator for initial identification and authentication, and documented in SSP. Group authenticators may not be shared with anyone outside of the group.

Section 6. Protection Requirements

8-600. Introduction. This section describes the implementation requirements for different protection measure.

8-601. Alternate Power Source (Power). An alternate power source ensures that the system availability is maintained in the event of a loss of primary power. An APS can also provide a time period for orderly system shutdown or the transfer of system operations to another system or power source.

a. **Power 1 Requirements.** Procedures for the graceful shutdown of the system shall ensure no loss of data. The decision not to use an alternate source of power, such as an uninterruptible power supply (UPS) for the system, shall be documented.

b. **Power 2 Requirements.** Instead of Power 1, procedures for transfer of the system to another power source shall ensure that the transfer is completed within the time requirements of the application(s) on the system.

8-602. Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.

a. **Audit 1 Requirements**

(1) Automated Audit Trail Creation: The system shall automatically create and maintain an audit trail or log (On a PL-1 system only: In the event that the Operating System cannot provide an automated audit capability, an alternative method of accountability for user activities on the system shall be developed and documented.) Audit records shall be created to record the following:

(a) Enough information to determine the date and time of action (e.g., common network time), the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved.

(b) Successful and unsuccessful logons and logoffs.

(c) Successful and unsuccessful accesses to security-relevant objects and directories, including creation, open, close, modification, and deletion.

(d) Changes in user authenticators.

(e) The blocking or blacklisting of a user ID, terminal, or access port and the reason for the action.

(f) Denial of access resulting from an excessive number of unsuccessful logon attempts.

(2) Audit Trail Protection. The contents of audit trails shall be protected against unauthorized access, modification, or deletion.

(3) Audit Trail Analysis. Audit analysis and reporting shall be scheduled, and performed. Security relevant events shall be documented and reported. The frequency of the review shall be at least weekly and shall be documented in the SSP.

(4) Audit Record Retention. Audit records shall be retained for at least one review cycle or as required by the CSA.

b. **Audit 2 Requirements.** In addition to Audit 1:

(1) Individual accountability (i.e., unique identification of each user and association of that identity with all auditable actions taken by that individual). Periodic testing by the ISSO or ISSM of the security posture of the IS

c. **Audit 3 Requirements.** In addition to Audit 2:

(1) Automated Audit Analysis. Audit analysis and reporting using automated tools shall be scheduled and performed.

d. **Audit 4 Requirements.** In addition to Audit 3:

(1) An audit trail, created and maintained by the IS, that is capable of recording changes to mechanism's list of user formal access permissions.

8-603. Backup and Restoration of Data (Backup). The regular backup of information is necessary to ensure that users have continuing access to the information. The periodic checking of backup inventory and testing of the ability to restore information validates that the overall backup process is working.

a. **Backup 1 Requirements**

(1) Backup Procedures. Procedures for the regular backup of all essential and security-relevant information, including software tables and settings, such as router tables, software, and documentation, shall be documented.

(2) Backup Frequency. The frequency of backups shall be defined by the ISSM, with the assistance of the GCA, and documented in the backup procedures.

b. **Backup 2** Requirements. In addition to Backup 1:

(1). Backup Media Storage. Media containing backup files and backup documentation shall be stored at another location, such as another part of the same building, a nearby building, or off facility, so as to reduce the possibility that a common occurrence could eliminate the on-facility backup data and the off-facility backup data.

(2) Verification of Backup Procedures. Backup procedures shall be periodically verified.

c. **Backup 3 Requirements.** In addition to Backup 2:

(1) Information Restoration Testing. Incremental and complete restoration of information from backup media shall be tested on an annual basis.

8-604. Changes to Data (Integrity). The control of changes to data includes deterring, detecting, and reporting of successful and unsuccessful attempts to change data. Control of changes to data may range from simply detecting a change attempt to the ability to ensure that only authorized changes are allowed.

a. **Integrity 1 Requirements**

(1) Change Procedures. Procedures and technical system features shall be implemented to ensure that changes to the data and IS software are executed only by authorized personnel or processes.

b. **Integrity 2 Requirements.** In addition to Integrity 1:

(1) Transaction Log. A transaction log, protected from unauthorized changes, shall be available to allow the immediate correction of unauthorized data and IS software changes and the off-line verification of all changes at all times.

8-605. Data Transmission (Trans). Information protection is required whenever classified information is to be transmitted through areas or components where individuals not authorized to have access to the information may have unescorted physical or uncontrolled electronic access to the information or communications media (e.g., outside the system perimeter).

a. **Trans 1 Requirements**

(1) Protections. One or more of the following protections shall be used.

(a) Information distributed only within an area approved for open storage of the information.

(b) NSA-approved encryption mechanisms appropriate for the encryption of classified information.

(c) Protected Distribution System.

8-606. Access Controls (Access). The IS shall store and preserve the integrity of the sensitivity of all information internal to the IS.

a. **Access 1 Requirements**

(1) Denial of physical access by unauthorized individuals unless under constant supervision of technically qualified, authorized personnel.

b. **Access 2 Requirements.** In addition to Access 1:

(1) Discretionary access controls shall be provided. A system has implemented discretionary access controls when the security support structure defines and controls access between named users and named objects (e.g., files and programs) in the system. The discretionary access control policy includes administrative procedures to support the policy and its mechanisms.

c. **Access 3 Requirements.** In addition to Access 2:

(1) Some process or mechanism that allows users (or processes acting on their behalf) to determine the formal access approvals granted to another user.

(2) Some process or mechanism that allows users (or processes acting on their behalf) to determine the sensitivity level of data.

8-607. Identification and Authentication (I&A)

a. **I&A 1Requirements.** Procedures that include provisions for uniquely identifying and authenticating the users. Procedures can be external to the IS (e.g., procedural or physical controls) or internal to the IS (i.e., technical). Electronic means shall be employed where technically feasible.

b. **I&A 2 Requirements.** In addition to I&A 1:

(1) An I&A management mechanism that ensures a unique identifier for each user and that associates that identifier with all auditable actions taken by the user. The following must be specified in the SSP:

(a) Initial authenticator content and administrative procedures for initial authenticator distribution.

(b) Individual and Group Authenticators. Group authenticators may only be used in conjunction with an individual/unique authenticator, that is, individuals must be authenticated with an individual authenticator prior to use of a group authenticator.

(c) Length, composition and generation of authenticators.

(d) Change processes (periodic and in case of compromise.

(e) Aging of static authenticators (i.e., not one-time passwords or biometric patterns).

(f) History of authenticator changes, with assurance of non-replication of individual authenticators.

(g) Protection of authenticators.

c. **I&A 3 Requirements.** In addition to I&A 2:

(1) Access to the IS by privileged users who either reside outside of the IS's perimeter or whose communications traverse data links that are outside the IS's perimeter shall require the use of strong authentication (i.e., an I&A technique that is resistant to replay attacks.)

d. **I&A 4 Requirements.** In those instances where the means of authentication is user-specified passwords, the ISSM may employ (with the approval of the CSA) automated tools to validate that the passwords are sufficiently strong to resist cracking and other attacks intended to discover the user's password.

e. **I&A 5 Requirements.** In those instances where the users are remotely accessing the IS, the users shall employ a strong authentication mechanism.

8-608. Resource Control (ResrcCtrl) The system shall ensure that resources contain no residual data before being assigned, allocated, or reallocated.

8-609. Session Controls (SessCtrl). Session controls are requirements, over and above identification and authentication, for controlling the establishment of a user’s session.

a. **SessCtrl 1 Requirements**

(1) User Notification. All users shall be notified prior to gaining access to a system that system usage is monitored, recorded, and subject to audit. The user shall also be advised that, by using the system, he/she has granted consent to such monitoring and recording. The user shall also be advised that unauthorized use is prohibited and subject to criminal and civil penalties. If the operating system permits, each initial screen (displayed before user logon) shall contain a warning text to the user and the user shall be required to take positive action to remove the notice from the screen (monitoring and recording, such as collection and analysis of audit trail information, shall be performed). The CSA will provide an approved banner. If it is not possible to provide an “initial screen” warning notice, other methods of notification shall be developed and approved by the CSA.

(2) Successive Logon Attempts. If the operating system provides the capability, successive logon attempts shall be controlled as follows:

(a) By denying access after multiple (maximum of five) consecutive unsuccessful attempts on the same user ID.

(b) By limiting the number of access attempts in a specified time period.

(c) By the use of a time delay control system.

(d) By other such methods, subject to approval by the CSA.

(3) System Entry. The system shall grant system entry only in accordance with the conditions associated with the authenticated user's profile. If no explicit entry conditions are defined, the default shall prohibit all remote activities, such as remote logons and anonymous file access.

b. **SessCtrl 2 Requirements.** In addition to SessCtrl 1:

(1). Multiple Logon Control. If the IS supports multiple logon sessions for each user ID or account, the IS shall provide a protected capability to control the number of logon sessions for each user ID, account, or specific port of entry. The IS default shall be a single logon session.

(2). User Inactivity. The IS shall detect an interval of user inactivity, such as no keyboard entries, and shall disable any future user activity until the user re-establishes the correct identity with a valid authenticator. The inactivity time period and restart requirements shall be documented in the SSP.

(3). Logon Notification. If the operating system provides the capability, the user shall be notified upon successful logon of: the date and time of the user's last logon; the location of the user (as can best be determined) at last logon; and the number of unsuccessful logon attempts using this user ID since the last successful logon. This notice shall require positive action by the user to remove the notice from the screen.

8-610. Security Documentation (Doc). Security documentation includes all descriptions of the security features, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system, or update to an existing system, meets the protection profile requirements. The SSP is used throughout the certification and approval process and serves for the lifetime of the system as the formal record of the system and its environment as approved for operation. The SSP also serves as the basis for inspections of the system. Information common to several systems at a facility or information contained in other documents may be attached to or referenced in the SSP.

a. **Doc 1 Requirements**

(1) SSP. The SSP shall contain the following:

(a) System Identification.

1. Security Personnel. The name, location, and phone number of the responsible system owner, CSA, ISSM, and ISSO.

2. Description. A brief narrative description of the system or network mission or purpose and architecture, including subnetworks, communications devices, and protocols.

(b) System Requirements Specification.

1. Sensitivity and Classification Levels. The sensitivity or classification levels, and categories of all information on the system and clearance, formal access approval and need-to-know of IS users.

2. Levels of Concern for Confidentiality, Integrity, and Availability. The confidentiality level of concern and protection level, the integrity level of concern, and the availability level of concern.

3. Protection Measures. Identify protection measures and how they are being met.

4. Variances from Protection Measure Requirements. A description of any approved variances from protection measures. A copy of the approval documentation shall be attached to the SSP.

(c) System-Specific Risks and Vulnerabilities. A description of the risk assessment of any threats or vulnerabilities unique to the system. If there are no threats or vulnerabilities unique to the facility or system, a statement to that effect shall be entered. If any vulnerabilities are identified by the assessment of

unique threats, the countermeasures implemented to mitigate the vulnerabilities shall be described.

(d) System Configuration. A brief description of the system architecture, including a block diagram of the components that show the interconnections between the components and any connections to other systems, and an information flow diagram.

(e) Connections to Separately Accredited Networks and Systems. If connections to other systems exist, a memorandum of understanding is necessary if the systems are approved by a person other than the CSA responsible for this system. A copy of any memoranda of understanding with other agencies shall be attached to the SSP.

(f) Security Support Structure. A brief description of the security support structure including all controlled interfaces, their interconnection criteria, and security requirements.

(2) Certification and Accreditation Documentation.

(a) Security Testing. Test plans, procedures, and test reports including risk assessment.

(b) Documentation. The test plan for ongoing testing and the frequency of such testing shall be documented in the SSP.

(c) Certification. A certification statement that the system complies with the requirements of the protection level and levels of concern for this system. The statement shall be signed by the ISSM.

(d) Accreditation. Documentation for accreditation includes the certification package. The CSA approves the package and provides accreditation documentation.

8-611. Separation of Function Requirements (Separation). At Protection Level 3 the functions of the ISSO and the system manager shall not be performed by the same person.

8-612. System Recovery (SR). System recovery addresses the functions that respond to failures in the SSS or interruptions in operation. Recovery actions ensure that the SSS is returned to a condition where all security-relevant functions are operational or system operation is suspended.

a. **SR 1 Requirements.** Procedures and IS features shall be implemented to ensure that IS recovery is done in a controlled manner. If any off-normal conditions arise during recovery, the IS shall be accessible only via terminals monitored by the ISSO or his /her designee, or via the IS console.

8-613. System Assurance (SysAssur). System assurance includes those components of a system (hardware, software, firmware, and communications) that are essential to maintaining the security policy(ies) of the system, (e.g. Security Support Structure).

a. **SysAssur 1 Requirements**

(1) Access to Protection Functions. Access to hardware/software/firmware that perform systems or security functions shall be limited to authorized personnel.

b. **SysAssur 2 Requirements.** In addition to SysAssur1:

(1) Protection Documentation. The protections and provisions of the SysAssur shall be documented.

(2) Periodic Validation of SysAssur.

Features and procedures shall exist to

periodically validate the correct operation of the

hardware, firmware, and software elements of

the SSS and shall be documented in the SSP.

c. **SysAssur 3 Requirements.** In addition to SysAssur2:

(1) SSS Isolation. The SSS shall maintain a domain for its own execution that protects it from external interference and tampering (e.g., by reading or modifying its code and data structures).

8-614. Security Testing (Test). Certification and ongoing security testing are the verification of correct operation of the protection measures in a system. The ISSM will perform and document the required tests.

a. **Test 1 Requirements.** Assurance shall be provided to the CSA that the system operates in accordance with the approved SSP and that the security features, including access controls and configuration management, are implemented and operational.

b. **Test 2 Requirements.** In addition to Test1:

(1) Written assurance shall be provided to the CSA that the IS operates in accordance with the approved SSP, and that the security features, including access controls, configuration management and discretionary access controls, are implemented and operational.

c. **Test 3 Requirements.** In addition to Test2:

(1) Certification testing shall be conducted including verification that the features and assurances required for the Protection Level are functional.

(a) A test plan and procedures shall be developed and shall include:

1. A detailed description of the manner in which the system's Security Support Structure meets the technical requirements for the Protection Levels and Levels-of-Concern for integrity and availability.

2. A detailed description of the assurances that have been implemented, and how this implementation will be verified.

3. An outline of the inspection and test procedures used to verify this compliance.

8-615. Disaster Recovery Planning. If disaster recovery planning is contractually mandated, the ISSM will develop a plan that identifies the facility's mission essential applications and information, procedures for the backup of all essential information and software on a regular basis, and testing procedures.

Section 7. Interconnected Systems

8-700. Interconnected Systems Management. The characteristics and capabilities of an IS implemented as networks require special security considerations. This section states additional requirements on a network or expands on the security requirements stated in Section 6 as they apply to a network.

a. When connecting two or more networks, the CSA shall review the security attributes of each network (even if the networks are accredited at the same protection level) to determine whether the combination of data and/or the combination of users on the connected network requires a higher protection level.

b. A unified network is a connected collection of systems or networks that are accredited: (1) under a single SSP, (2) as a single entity, and (3) by a single CSA. Such a network can be as simple as a small stand-alone LAN operating at Protection Level 1, following a single security policy, accredited as a single entity, and administered by a single ISSO. Conversely, it can be as complex as a collection of hundreds of LANs separated over a wide area but still following a single security policy, accredited as a single entity by a single CSA. The perimeter of each network encompasses all its hardware, software, and attached devices. Its boundary extends to all of its users.

c. An interconnected network is comprised of two or more separately accredited systems and/or networks. Each separately accredited system or network maintains its own intra-system services and controls, protects its own resources, and retains its individual accreditation. Each participating system or network has its own ISSO. The interconnected network shall have a controlled interface capable of adjudicating the different security policy implementations of the participating systems or unified networks. An interconnected network also requires accreditation as a unit.

d. Systems that process information at differing classification levels or with differing compartmentation (i.e., at least two kinds of information that require different formal access approvals) can be interconnected if:

(1) They are interconnected through a Controlled Interface (as defined below) that provides the separation appropriate to the combination of the level(s) and compartment(s) being processed on both systems; or

(2) Both systems are operating at the same protection level (both systems must be accredited to protect the information being transferred); or

(3) Both systems are accredited to process the level(s) and compartment(s) of information that they will receive, and at least one system is accredited to provide appropriate separation for the information being transferred.

e. Any IS connected to another system that does not meet either d (2) or d (3) above shall utilize a Controlled Interface(s) (CI) that performs the following:

(1) A communication of lower classification level from within the system perimeter shall be reviewed for classification before being released.

(2) A classified communication from within the system perimeter shall have the body and attachments of the communication encrypted with the appropriate level of encryption for the information, transmission medium, and target system.

(3) Communications from outside the system perimeter shall have an authorized user as the addressee (i.e., the CI shall notify the user of the communication and forward the communication only on request from the user). If classified information exists in the communication, it shall be encrypted with the appropriate level of encryption for the information, transmission medium, and target system.

8-701. Controlled Interface Functions

a. The functions of the CI include:

(1) Providing a secure point of interconnection between networks, connected peripheral devices, remote terminals, or remote hosts.

(2) Providing a reliable exchange of security-related information.

(3) Filtering information in a data stream based on associated security labels for data content.

b. CIs have several characteristics including the following:

(1) There are no general users on the CI.

(2) There is no user code running on the CI.

(3) The CI provides a protected conduit for the transfer of user data.

(4) Communications from outside the perimeter of the system shall be reviewed for viruses and other malicious code.

8-702. Controlled Interface Requirements. The CI shall have the following properties:

a. Adjudicated Differences. The CI shall be implemented to monitor and enforce the protection requirements of the network and to adjudicate the differences in security policies.

b. Routing Decisions. The CI shall base its routing decisions on information that is supplied or alterable only by the SSS.

c. Restrictive Protection Requirements. The CI shall support the protection requirements of the most restrictive of the attached networks or IS.

d. User Code. The CI shall not run any user code.

e. Fail-secure. The CI shall be implemented so that all possible failures shall result in no loss of confidentiality or unacceptable exposure to loss of integrity or availability.

f. Communication Limits. The CI shall ensure that communication policies and connections that are not explicitly permitted are prohibited.

g. In general, such systems have only privileged users; i.e., system administrators and maintainers. The CI may have a large number of clients (i.e., individuals who use the CI's functional capabilities in a severely constrained way). The CI application itself will have to provide the more stringent technical protections appropriate for the system's protection level. Multiple applications do not affect the overall protection provided by the CI if each application (and the resources associated with it) is protected from unauthorized access or circumvention from other applications or users.

8-703. Assurances for CIs. Each CI shall be tested and evaluated to ensure that the CI, as implemented, can provide the separation required for the system's protection level. Specifically, the platform on which the CI runs does not necessarily have to provide the needed separation alone

CHAPTER 9
Special Requirements

Section 1. RD and FRD

9-100. General. This section was prepared by DOE according to reference (a) and is provided for information purposes only. It describes the requirements for classifying and safeguarding nuclear-related information that is designated RD or FRD. Such information is classified under reference (c) as opposed to other Government information that is classified by E.O. (National Security Information (NSI)).

9-101. Authority and Responsibilities.

a. Reference (c) establishes policy for classifying and protecting RD and FRD information. Under section 141 of reference (c), DOE is responsible for controlling the dissemination and declassification of RD. Under section 142c and d of reference (c), DOE shares certain responsibilities regarding RD and FRD with the Department of Defense. Under section 142e of reference (c), DOE shares certain responsibilities regarding RD with the DNI. Under section 143 of reference (c), the Secretary of Defense is responsible for establishing personnel and other security procedures and standards that are in reasonable conformity to the standards established by DOE. The procedures and standards established by the Secretary of Defense are detailed in other sections of the Manual and are applicable to contractors under the security cognizance of the Department of Defense.

b. Specific policies and procedures for classifying and declassifying RD and FRD are set forth in 10 Code of Federal Regulations (CFR) Part 1045, Subparts A, B, and C (reference (q)).

c. The Secretary of Energy and the Chairman of the NRC retain authority over access to information that is under their respective cognizance as directed by reference (c). The Secretary of DOE or the Chairman of the NRC may inspect and monitor contractor programs or facilities that involve access to such information or may enter into written agreement with the Department of Defense to inspect and monitor these programs or facilities.

9-102. Unauthorized Disclosures. Contractors shall report all unauthorized disclosures involving RD and FRD information to the CSA.

9-103. International Requirements. Reference (c) provides for a program of international cooperation to promote common defense and security and to make available to cooperating nations the benefits of peaceful applications of atomic energy as widely as expanding technology and considerations of the common defense and security will permit. Under section 123 of reference (c), information controlled by reference (c) may be shared with another nation only under the terms of an agreement for cooperation. The disclosure by a contractor of RD and FRD shall not be permitted until an agreement is signed by the United States and participating governments and disclosure guidance and security arrangements are established. RD and FRD shall not be transmitted to a foreign national or regional defense organization unless such action is approved and undertaken under an agreement for cooperation between the United States and the cooperating entity and supporting statutory determinations as prescribed in reference (c).

9-104. Personnel Security Clearances. Only DOE, NRC, Department of Defense, and NASA can grant access to RD and FRD. The minimum investigative requirements and standards for access to RD and FRD for contractors under the security cognizance of DOE are set forth below.

a. TOP SECRET RD – A favorable SSBI.

b. SECRET RD – A favorable SSBI.

c. CONFIDENTIAL RD – A favorable NACLC.

d. TOP SECRET FRD – A favorable SSBI.

e. SECRET FRD – A favorable NACLC.

f. CONFIDENTIAL FRD – A favorable NACLC.

9-105. Classification.

a. The Director, DOE, Office of Classification and Information Control, determines whether nuclear-related information is classified as RD under reference (q). DOE and the Department of Defense

jointly determine what classified information is removed from the RD category to become FRD under section 14(a) of reference (q). These decisions are promulgated in classification guides issued under section 37(a) of reference (q).

b. Reference (q) describes the authorities and procedures for classifying RD and FRD information and documents. All contractors with access to RD and FRD shall designate specified employees as RD Classifiers. Only those contractor employees designated as RD classifiers may classify RD and FRD documents according to section 32(a)(2) of reference (q). Such employees must be trained on the procedures for classifying, declassifying, marking, and handling for RD and FRD information and documents according to section 35(a) of reference (q). RD classifiers shall use classification guides as the primary basis for classifying and declassifying documents containing RD and FRD information according to section 37(c) of reference (q). If such classification guidance is not available and the information in the document appears to meet the definition of RD, then the RD classifier shall, as an interim measure, mark the document as Confidential RD (or as Secret RD if the sensitivity of the information in the document so warrants) and promptly forward the document to the GCA. The GCA shall provide the contractor with the final determination based upon official published classification guidance. If the GCA cannot make such a determination, the GCA shall forward the document to DOE for a classification determination according to section 14(a) of reference (q).

c. Classifying information as RD and FRD is not limited to U.S. Government information. Contractors who develop an invention or discovery useful in the production or utilization of special nuclear material or nuclear energy shall file a fully descriptive report with DOE or the Commissioner of Patents as prescribed by Section 151c of reference (c). Documents thought to contain RD or FRD shall be marked temporarily as such. These documents shall be promptly referred to the GCA for a final determination based upon official published classification guidance. If the GCA cannot make such a determination, the GCA shall forward the document to DOE for a classification determination.

9-106. Declassification.

a. DOE determines whether RD information may be declassified under section 14(b) of reference (q). DOE, jointly with the Department of Defense, determines whether FRD information may be declassified under section 14(d) of reference (q).

b. Documents marked as containing RD and FRD information remain classified until a positive action by an authorized Government official is taken to declassify them; no date or event for automatic declassification ever applies to RD and FRD documents.

9-107. Challenges to RD/FRD Classification. Any contractor employee who believes that an RD/FRD document is classified improperly or unnecessarily may challenge that classification following the procedures established by the GCA.

9-108. Marking. Documents containing RD and FRD information shall be marked as indicated below:

a. Front of the Document. In addition to the overall classification level of the document at the top and bottom of the page, the following notices must appear on the front of the document, as appropriate:

If the document contains RD information:

> RESTRICTED DATA
> This document contains RESTRICTED DATA as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

If the document contains FRD information:

> FORMERLY RESTRICTED DATA
> Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144b, AEA 1954.

A document containing RD or FRD information also must be marked to identify: (1) the classification guide or source document (by title and date) used to classify the document and (2) the identity of the RD classifier unless the classifier is the same as the document originator or signer:

> Derived from: (Classification guide or source document – title and date)
> RD Classifier: (Name and position or title)

b. Interior Page. Each RD or FRD document must also be clearly marked at the top and bottom of each interior page with the overall classification level and category of the document or the classification level and category of the page, whichever is

preferred. The abbreviations RD and FRD may be used in conjunction with the classification level (e.g., SECRET RD or SECRET FRD).

c. Other Caveats. Any other caveats indicated on the source document shall be carried forward.

Section 2. DOD Critical Nuclear Weapon Design Information (CNWDI)

9-200. General. This section contains the special requirements for protection of CNWDI.

9-201. Background. CNWDI is a DoD category of TOP SECRET RD or SECRET RD that reveals the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition munition, or test device. Specifically excluded is information concerning arming, fuzing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive materials by type. Among these excluded items are the components that DoD personnel set, maintain, operate, test or replace. The sensitivity of DoD CNWDI is such that access shall be granted to the absolute minimum number of employees who require it for the accomplishment of assigned responsibilities on a classified contract. Because of the importance of such information, special requirements have been established for its control. DoD Directive 5210.2 (reference (r)) establishes these controls in DoD.

9-202. Briefings. Prior to having access to DoD CNWDI, employees shall be briefed on its sensitivity by the FSO or his or her alternate. (The FSO will be initially briefed by a Government representative.) The briefing shall include the definition of DoD CNWDI, a reminder of the extreme sensitivity of the information, and an explanation of the individual's continuing responsibility for properly safeguarding DoD CNWDI, and for ensuring that dissemination is strictly limited to other personnel who have been authorized for access and have a need-to-know for the particular information. The briefing shall also be tailored to cover any special local requirements. Upon termination of access to DoD CNWDI, the employee shall be given an oral debriefing.

9-203. Markings. In addition to any other required markings, CNWDI material shall be clearly marked, "Critical Nuclear Weapon Design Information-DoD Directive 5210.2 Applies." As a minimum, CNWDI documents shall show such markings on the cover or first page. Portions of documents that contain CNWDI shall be marked with an (N) or (CNWDI) following the classification of the portion; for example, TS(RD)(N) or TS(RD)(CNWDI).

9-204. Subcontractors. Contractors shall not disclose CNWDI to subcontractors without the prior written approval of the GCA. This approval may be included in a Contract Security Classification Specification, other contract-related document, or by separate correspondence.

9-205. Transmission Outside the Facility. Transmission outside the contractor's facility is authorized only to the GCA, or to a subcontractor as described in paragraph 9-204 above. Any other transmission must be approved by the GCA. Prior to transmission to another cleared facility, the contractor shall verify from the CSA that the facility has been authorized access to CNWDI. When CNWDI is transmitted to another facility, the inner wrapping shall be addressed to the personal attention of the FSO or his or her alternate, and in addition to any other prescribed markings, the inner wrapping shall be marked: "Critical Nuclear Weapon Design Information-DoD Directive 5210.2 Applies." Similarly, transmissions addressed to the GCA or other U.S. Government agency shall bear on the inner wrapper the marking "Critical Nuclear Weapon Design Information-DoD Directive 5210.2 Applies."

9-206. Records. Contractors shall annotate CNWDI access in the CSA-designated database for all employees who have been authorized access to CNWDI.

9-207. Weapon Data. That portion of RD or FRD that concerns the design, manufacture, or utilization (including theory, development, storage, characteristics, performance, and effects) of atomic weapons or atomic weapon components and nuclear explosive devices is called Weapon Data and it has special protection provisions. Weapon Data is divided into Sigma categories the protection of which is prescribed by DOE Order 5610.2 (reference (s)). However, certain Weapon Data has been re-categorized as CNWDI and is protected as described in this section.

Section 3. Intelligence Information

9-300. Background. This section was prepared by CIA in accordance with reference (a) and is provided for information purposes only. It contains general information on safeguarding intelligence information. Intelligence information is under the jurisdiction and control of the DNI, who establishes security policy for the protection of intelligence information, sources, methods, and analytical processes.

9-301. Definitions. The following definitions pertain to intelligence information:

a. Counterintelligence (CI). Information collection, analysis and operations conducted to identify and neutralize espionage, other foreign intelligence or covert actions, the intelligence-related capabilities and activities of terrorists, and operations against U.S. personnel or political, economic and policy processes.

b. Classified Intelligence Information. Information identified as SCI included in SAPs for intelligence, and collateral classified intelligence information under the purview of the DNI.

c. Foreign Intelligence. Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence information except for information on international terrorist activities.

d. Intelligence Community (IC). Those U.S. Government organizations and activities identified as members of the IC in reference (h).

e. Senior Officials of the Intelligence Community (SOICs). SOICs are the heads of departments and agencies with organizations in the IC or the heads of IC organizations responsible for protecting classified intelligence information and intelligence sources and methods from unauthorized disclosure consistent with DNI policy.

f. Senior Intelligence Officer (SIO). The SIO is the highest ranking military or civilian individual charges with direct foreign intelligence missions, functions, or responsibilities within an element of the IC.

g. SCI. SCI is classified intelligence information concerning or derived from sensitive sources, methods, or analytical processes, which is required to be handled exclusively within formal access control systems established by the DNI.

h. SCI Facility (SCIF). A SCIF is an area, room, group of rooms, or installation accredited by the proper authority to store, use, discuss and/or process SCI.

9-302. Key Concepts. This section provides general guidance on the intended purpose of several security tenets that form a critical baseline for the protection of intelligence information.

a. Apply Need-to-Know. Authorized holders (individuals or information systems) of classified intelligence information shall determine if prospective recipients (individuals or information systems) have the requisite clearances and accesses, and require knowledge of specific classified intelligence information in order to perform or assist in a lawful and authorized governmental function. To effectively implement this concept, IC departments, agencies, and bureaus must work cooperatively with customers to understand their requirements and ensure that they receive all applicable classified intelligence information while minimizing the risk of unauthorized disclosure. IC organizations shall provide intelligence at multiple security levels appropriate to the security authorizations of intended customers. Customers, in turn, shall be responsible for verifying need-to-know for this information for individuals of information systems within their organizations.

b. Protect SCI. In order to protect information regarding particularly fragile intelligence sources and methods, SCI has been established as the SAP for the DNI. SCI must be protected in specific SCI control systems and shall be clearly defined and identified. The DNI has the sole authority to create or to discontinue SAPs, including SCI access control systems pertaining to intelligence sources and methods and classified intelligence activities (including special activities, but not including military operational, strategic, and tactical programs).

c. Educate the Work Force. SOICs shall establish formal security awareness training and education programs to ensure complete, common, and consistent understanding and application of security principles. Individuals shall be advised of their security responsibilities before receiving access

to classified intelligence information and information systems. Annual refresher training is required to review security principles and responsibilities and to emphasize new security policies and practices developed from the preceding year.

d. Promote Security Reciprocity. To facilitate security reciprocity across the IC and industry, SOICs shall accept from other IC departments, agencies, and bureaus access eligibility determinations and accreditations of information systems and facilities except when an agency has documented information indicating that an employee, contractor, information system, or a facility does not meet DCID standards. Any exceptions to access eligibility determinations and accreditations of information systems and facilities must be noted in certifications to other agencies.

e. Promote Institutional Collaboration. Security elements of the IC shall work with intelligence production, counterintelligence, and law enforcement partners to identify and implement integrated responses to threats. Proactive collaboration among programs should synergize efforts to protect the U.S. population, national security assets, and classified intelligence information.

f. Manage Risk. IC departments, agencies and bureaus shall employ a risk management/risk analysis process to cost-effectively minimize the potential for loss of classified intelligence information or assets and the consequences should such loss occur. This methodology shall involve techniques to counter threats, reduce vulnerabilities, and implement security countermeasures.

g. Minimize Insider Threat. All personnel who have access to classified intelligence information shall be thoroughly vetted, fully trained in their security responsibilities, appropriately supervised, and provided a secure work environment. CI and security management shall maintain aggressive programs to deter, detect, and support the apprehension and prosecution of those cleared personnel who endanger national security interests.

9-303 Control Markings Authorized for Intelligence Information

a. "DISSEMINATION AND EXTRACTION OF INFORMATION CONROLLED BY ORIGINATOR" (ORCON). Information bearing this marking may be disseminated within the headquarters and specified subordinate elements of the recipient organizations, including their contractors within government facilities. This information may also be incorporated in whole or in part into other briefings or products, provided the briefing or product is presented or distributed only to original recipients of the information and marked accordingly. Dissemination beyond headquarters and specified subordinate elements or to agencies other than the original recipients requires advanced permission from the originator.

b. "FOR OFFICIAL USE ONLY" (FOUO). Intelligence information used to control dissemination of UNCLASSIFIED official government information until approved for public release by the originator. May be used only with UNCLASSIFIED on page markings.

c. "CAUTION-PROPRIETARY INFORMATION INVOLVED" (PROPIN). Marking used to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a proprietary trade secret or proprietary data believed to have actual or potential value. This information may not be disseminated outside the Federal Government in any form without the express permission of the originator of the proprietary information. Dissemination to contractors is precluded irrespective of their status to, or within, the U.S. Government without the authorization of the originator of the information.

d. "NOT RELEASABLE TO FOREIGN NATIONALS" (NOFORN). NOFORN is classified information that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-U.S. citizens without permission of the originator. It cannot be used with REL TO [country codes] or EYES ONLY on page markings. When a document contains both NOFORN and REL TO (see below) or NOFORN and EYES ONLY portions, NOFORN takes precedence for the markings at the top and bottom of the page.

e. "AUTHORIZED FOR RELEASE TO (REL TO) (name of country (ies)/international organization)". This marking is used to identify Intelligence Information that an originator has predetermined to be releasable or has released, through established foreign disclosure procedures and channels, to the foreign/international organization indicated.

9-304. Limitation on Dissemination of Classified Intelligence Information. A contractor is not

authorized to further disclose or release classified intelligence information (including release to a subcontractor) without prior written authorization of the releasing agency.

9-305. Safeguarding Classified Intelligence Information. All classified intelligence information in the contractor's possession shall be safeguarded and controlled according to the provisions of this manual for classified information of the same classification level, with any additional requirements and instructions received from the GCA, and with any specific restrictive markings or limitations that appear on the documents themselves.

9-306. Inquiries. All inquiries concerning source, acquisition, use, control, or restrictions pertaining to classified intelligence information shall be directed to the providing agency.

Section 4. Communications Security (COMSEC)

9-400. General. This section was prepared by NSA. The procedures in this section pertaining to COMSEC information shall apply to contractors when the contractor requires the use of COMSEC systems in the performance of a contract; the contractor is required to install, maintain, or operate COMSEC equipment for the U.S. Government; or the contractor is required to accomplish research, development, or production of COMSEC systems, COMSEC equipment, or related COMSEC material.

9-401. Instructions. Specific requirements for the management and safeguarding of COMSEC material in industry are established in the COMSEC material control and operating procedures provided to the custodian of each industrial COMSEC account by the agency Central Office of Record (COR) responsible for establishing the account. Such procedures that are above the baseline requirements detailed in the other sections of this manual shall be contractually mandated.

9-402. Clearance and Access Requirements

a. 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 have a final PCL appropriate for the material to be held in the account. COMSEC custodians and alternate COMSEC custodians having access to TOP SECRET keying material marked as containing CRYPTOGRAPHIC (CRYPTO) information must have a final security clearance based upon an SSBI current within five years. This requirement does not apply to contractors using only data transfer devices and seed key.

b. Before disclosure of COMSEC information to a contractor, GCAs must first verify with the CSA that appropriate COMSEC procedures are in place at the contractor facility. If procedures are not in place, the GCA shall provide a written request and justification to the CSA to establish COMSEC procedures and a COMSEC account, if appropriate, at the facility and to conduct the initial COMSEC briefings for the FSO and custodians.

c. Access to COMSEC information by a contractor requires a final FCL and a government-issued final PCL at the appropriate level; however, an Interim TOP SECRET FCL or PCL is valid for access to COMSEC at the SECRET and CONFIDENTIAL levels.

d. If a COMSEC account will be required, the Contract Security Classification Specification shall contain a statement regarding the establishment of a COMSEC account as appropriate.

9-403. Establishing a COMSEC Account

a. When COMSEC material which is accountable to a COR is to be provided, acquired or produced under a contract, the contracting officer shall inform the contractor that a COMSEC account must be established. The contractor shall forward the names of U.S. citizen employees who will serve as the COMSEC Custodian and Alternate COMSEC Custodian to the CSA. The CSA shall forward the names of the FSO, COMSEC Custodian, and Alternate Custodian to the appropriate COR, with a copy to the GCA, indicating that the persons have been cleared and COMSEC has been briefed.

b. The COR will then establish the COMSEC account and notify the CSA that the account has been established.

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

9-404. COMSEC Briefing and Debriefing Requirements

a. All contractor employees who require access to classified COMSEC information in the performance of their duties shall be briefed before access is granted. Depending on the nature of COMSEC access required, either a COMSEC briefing or a Cryptographic Access Briefing will be given. The FSO, the COMSEC Custodian, and the Alternate Custodian shall be briefed by a government representative or their designee. Other contractor employees shall be briefed by the FSO, the COMSEC Custodian, the Alternate Custodian, or other individual designated by the FSO. The purpose of the briefing is to ensure that the contractor 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 (t)) for willful disclosure of COMSEC information.

b. COMSEC debriefings are not required.

c. The contractor shall maintain a record of all COMSEC briefings.

9-405. CRYPTO Access Briefing and Debriefing Requirements

a. U.S. classified CRYPTO information is defined as:

(1) TOP SECRET and SECRET, CRYPTO, key and authenticators that are designated CRYPTO, and

(2) CRYPTO media that embody, describe, or implement classified CRYPTO logic; this includes full maintenance manuals, CRYPTO descriptions, drawings of a CRYPTO logic, specifications describing a CRYPTO logic, CRYPTO computer software, or any other media which may be specifically identified.

b. U.S. classified CRYPTO information does not include seed key and CCI.

c. A contractor's employee may be granted access to U.S. classified CRYPTO information only if the employee:

(1) Is a U.S. citizen;

(2) Has a final government-issued security clearance appropriate to the classification of the U.S. CRYPTO information to be accessed;

(3) Has a valid need-to-know to perform duties for, or on behalf of, the U.S. Government;

(4) Receives a security briefing appropriate to the U.S. classified CRYPTO information to be accessed;

(5) Acknowledges the granting of access by executing Section I of Secretary of Defense Form (SD) 572, Cryptographic Access Certification and Termination; and

(6) Where so directed by a U.S. Government Department or Agency head, acknowledges the possibility of being subject to a non-lifestyle, CI-scope polygraph examination that shall be administered in accordance with department or agency directives and applicable law.

d. An employee granted access to CRYPTO information shall be debriefed and execute Section II of the SD 572 not later than 90 days from the date access is no longer required.

e. The contractor shall maintain the SD 572 for a minimum of three years following the debriefing.

f. CRYPTO access briefings fully meet the requirements of paragraph 9-407 of this manual for COMSEC briefings.

9-406. Destruction and Disposition of COMSEC Material. The COR shall 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.

9-407. Subcontracting COMSEC Work. Subcontracts requiring the disclosure of classified COMSEC information shall be awarded only upon the written approval of the GCA.

9-408. Unsolicited Proposals. Any unsolicited proposal for a COMSEC system, equipment, development, or study that may be submitted by a contractor to a government agency shall be forwarded to the Deputy Director, Information Systems Security, NSA, Fort George G. Meade, MD 20755-6000, for review and appropriate follow-up action.

CHAPTER 10
International Security Requirements

Section 1. General and Background Information

10-100. General. This Chapter provides policy and procedures governing the control of classified information in international programs.

10-101. Applicable Federal Laws. The transfer of articles and services and related technical data to a foreign person, within or outside the U.S., or the movement of such material or information to any destination outside the legal jurisdiction of the U.S. constitutes an export. Depending on the nature of the articles or data, most exports are governed by the Arms Export Control Act (AECA) (reference (u)), the Export Administration Act (EAA) (reference (v)), and reference (c).

10-102. Bilateral Security Agreements. Bilateral security agreements are negotiated with various foreign governments. Confidentiality requested by some foreign governments prevents a listing of the countries that have executed these agreements.

a. The General Security Agreement, negotiated through diplomatic channels, requires that each government provide to the classified information provided by the other substantially the same degree of protection as the releasing government. The Agreement contains provisions concerning limits on the use of each government's information, including restrictions on third party transfers and proprietary rights. It does not commit governments to share classified information, nor does it constitute authority to release classified material to that government. It satisfies, in part, the eligibility requirements of reference (u) concerning the agreement of the recipient foreign government to protect U.S. classified defense articles and technical data. (The General Security Agreement also is known as a General Security of Information Agreement and General Security of Military Information Agreement. The title and scope are different, depending on the year the particular agreement was signed.)

b. Industrial security agreements have been negotiated with certain foreign governments that identify the procedures to be used when foreign government information is provided to industry. The Office of the Under Secretary of Defense (Policy) negotiates Industrial Security Agreements as an Annex to the General Security Agreement and the Director, DSS, has been delegated authority to implement the provisions of the Industrial Security Agreements. The Director of Security, NRC, negotiates and implements these agreements for the NRC.

Section 2. Disclosure of U.S. Information to Foreign Interests

10-200. Authorization for Disclosure. Disclosure guidance will be provided by the GCA. Disclosure authorization may be in the form of an export license, a technical assistance agreement, a manufacturing license agreement, a letter of authorization from the U.S. Government licensing authority, or an exemption to the export authorization requirements. Disclosure guidance provided for a previous contract or program shall not be used unless the contractor is so instructed in writing by the GCA or the licensing authority. Classified information normally will be authorized for disclosure and export as listed below:

a. Government-to-Government International Agreements. Classified information shall not be disclosed until agreements are signed by the participating governments and disclosure guidance and security arrangements are established. The export of technical data pursuant to such agreements may be exempt from licensing requirements of the International Traffic in Arms Regulation (ITAR) (reference (w).

b. Symposia, Seminars, Exhibitions, and Conferences. Appropriately cleared foreign nationals may participate in classified gatherings if authorized by the Head of the U.S. Government Agency that authorizes the conduct of the conference.

c. Foreign Visits. Disclosure of classified information shall be limited to that specific information authorized in connection with an approved visit request or export authorization.

d. Temporary Exports. Classified articles (including articles that require the use of classified information for operation) exported for demonstration purposes shall remain under U.S. control. The request for export authorization shall include a description of the arrangements that have been made in-country for U.S. control of the demonstrations and secure storage under U.S. Government control.

10-201. Direct Commercial Arrangements. The disclosure of classified information may be authorized pursuant to a direct commercial sale only if the proposed disclosure supports a U.S. or foreign government procurement requirement, a government contract, or an international agreement. A direct commercial arrangement includes sales, loans, leases, or grants of classified items, including sales under a government agency sales financing program. If a proposed disclosure is in support of a foreign government requirement, the contractor should consult with U.S. in-country officials (normally the U.S. Security Assistance/Armaments Cooperation Office or Commercial Counselor). An export authorization is required before a contractor makes a proposal to a foreign interest that involves the eventual disclosure of U.S. classified information. The contractor should obtain the concurrence of the GCA before submitting an export authorization request.

10-202. Contract Security Provisions.

a. When a U.S. contractor is authorized to award a subcontract or enter into a Manufacturing License Agreement, Technical Assistance Agreement, or other direct commercial arrangement with a foreign contractor that will involve classified information, security provisions will be incorporated in the subcontract document or agreement and security classification guidance via a Contract Security Classification Specification will be provided. A copy of the signed contract with the provisions and the classification guidance shall be provided to the CSA. If the export authorization specifies that additional security arrangements are necessary for performance on the contract, contractor developed arrangements shall be incorporated in appropriate provisions in the contract or in a separate security document.

b. The contractor shall prepare and maintain a written record that identifies the originator or source of classified information that will be used in providing defense articles or services to foreign customers. The contractor shall maintain this listing with the contractor's record copy of the pertinent export authorization.

c. Security provisions, substantially as shown below, shall be included in all contracts and subcontracts involving classified information that are awarded to foreign contractors.

(1) All classified information and material furnished or generated under this contract shall be protected as follows:

(a) The recipient will not release the information or material to a third-country government, person, or firm without the prior approval of the releasing government.

(b) The recipient will afford the information and material a degree of protection equivalent to that afforded it by the releasing government; and

(c) The recipient will not use the information and material for other than the purpose for which it was furnished without the prior written consent of the releasing government.

(2) Classified information and material furnished or generated under this contract shall be transferred through government channels or other channels specified in writing by the Governments of the United States and (insert applicable country) and only to persons who have an appropriate security clearance and an official need for access to the information in order to perform on the contract.

(3) Classified information and material furnished under this contract will be remarked by the recipient with its government's equivalent security classification markings.

(4) Classified information and material generated under this contract must be assigned a security classification as specified by the contract security classification specifications provided with this contract.

(5) All cases in which it is known or there is reason to believe that classified information or material furnished or generated under this contract has been lost or disclosed to unauthorized persons shall be reported promptly and fully by the contractor to its government's security authorities.

(6) Classified information and material furnished or generated pursuant to this contract shall not be further provided to another potential contractor or subcontractor unless:

(a) A potential contractor or subcontractor which is located in the United States or (insert applicable country) has been approved for access to classified information and material by U.S. or (insert applicable country) security authorities; or,

(b) If located in a third country, prior written consent is obtained from the United States Government.

(7) Upon completion of the contract, all classified material furnished or generated pursuant to the contract will be returned to the U.S. contractor or be destroyed.

(8) The recipient contractor shall insert terms that substantially conform to the language of these provisions, including this one, in all subcontracts under this contract that involve access to classified information furnished or generated under this contract.

Section 3. Foreign Government Information (FGI)

10-300. General. The contractor shall notify the CSA when awarded contracts by a foreign interest that will involve access to classified information. The CSA shall administer oversight and ensure implementation of the security requirements of the contract on behalf of the foreign government, including the establishment of channels for the transfer of classified material.

10-301. Contract Security Requirements. The foreign entity that awards a classified contract is responsible for providing appropriate security classification guidance and any security requirements clauses. The failure of a foreign entity to provide classification guidance shall be reported to the CSA.

10-302. Marking Foreign Government Classified Material.

a. Foreign government classified information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the government entity that furnished the information. The equivalent U.S. classification and the country of origin shall be marked on the front and back in English.

10-303. Foreign Government RESTRICTED Information and "In Confidence" Information.

a. Some foreign governments have a fourth level of classification that does not correspond to an equivalent U.S. classification that is identified as RESTRICTED Information. In many cases, bilateral security agreements require RESTRICTED information to be protected as U.S. CONFIDENTIAL information.

b. Some foreign governments may have a category of unclassified information that is protected by law. This latter category is normally provided to other governments on the condition that the information is treated "In Confidence." The foreign government or international organization must state that the information is provided in confidence and that it must be protected from release. A provision of Title 10 of the U.S. Code (reference (x)) protects information provided "In Confidence" by foreign governments or international organizations to the Department of Defense which is not classified but meets special requirements stated in section 130c reference (x). This provision also applies to RESTRICTED information which is not required by a bilateral agreement to be protected as classified information. The contractor shall not disclose information protected by this statutory provision to anyone except personnel who require access to the information in connection with the contract.

b. It is the responsibility of the foreign entity that awards the contract to incorporate requirements for the protection and marking of RESTRICTED or "In Confidence" information in the contract. The contractor shall advise the CSA if requirements were not provided by the foreign entity.

10-304. Marking U.S. Documents Containing FGI

a. U.S. documents containing foreign government information shall be marked on the front, "THIS DOCUMENT CONTAINS (indicate country of origin) INFORMATION." In addition, the portions shall be marked to identify both the country and classification level, e.g., (UK-C); (GE-C). The "Derived From" line shall identify U.S. as well as foreign classification sources.

b. If the identity of the foreign government must be concealed, the front of the document shall be marked "THIS DOCUMENT CONTAINS FOREIGN GOVERNMENT INFORMATION;" paragraphs shall be marked FGI, together with the classification level, e.g., (FGI-C); and the "Derived From" line shall indicate FGI in addition to any U.S. source. The identity of the foreign government shall be maintained with the record copy of the document.

c. A U.S. document, marked as described herein, shall not be downgraded below the highest level of foreign government information contained in the document or be declassified without the written approval of the foreign government that originated the information. Recommendations concerning downgrading or declassification shall be submitted to the GCA or foreign government contracting authority, as applicable.

10-305. Marking Documents Prepared For Foreign Governments. Documents prepared for foreign governments that contain U.S. and foreign government information shall be marked as prescribed by the foreign government. In addition, they shall be marked on the front, "THIS DOCUMENT CONTAINS UNITED STATES CLASSIFIED INFORMATION."

Portions shall be marked to identify the U.S. classified information.

10-306. Storage and Control. Foreign government material shall be stored and access shall be controlled generally in the same manner as U.S. classified material of an equivalent classification. Foreign government material shall be stored in a manner that will avoid commingling with other material which may be accomplished by establishing separate files in a storage container.

10-307. Disclosure and Use Limitations. Foreign government information is provided by the foreign government to the United States. It shall not be disclosed to nationals of a third country, or to any other third party, or be used for other than the purpose for which it was provided without the prior written consent of the originating foreign government. Requests for other uses or further disclosure shall be submitted to the GCA for U.S. contracts, and through the CSA for direct commercial contracts. Approval of the request by the foreign government does not eliminate the requirement for the contractor to obtain an export authorization.

10-308. Transfer. Foreign government information shall be transferred within the U.S. and its territories using the same channels as specified by this manual for U.S. classified information of an equivalent classification, except that non-cleared express overnight carriers shall not be used.

10-309. Reproduction. The reproduction of foreign government TOP SECRET information requires the written approval of the originating government.

10-310. Disposition. Foreign government information shall be destroyed on completion of the contract unless the contract specifically authorizes retention or return of the information to the GCA or foreign government that provided the information. TOP SECRET destruction must be witnessed and a destruction certificate executed and retained for 2 years.

10-311. Reporting of Improper Receipt of Foreign Government Material. The contractor shall report to the CSA the receipt of classified material from foreign interests that is not received through government channels.

10-312. Subcontracting

a. A U.S. contractor may award a subcontract that involves access to FGI to another U.S. contractor, except as described in subparagraph b, on verifying with the CSA that the prospective subcontractor has the appropriate FCL and storage capability. The contractor awarding a subcontract shall provide appropriate security classification guidance and incorporate the pertinent security provisions in the subcontract.

b. Subcontracts involving FGI shall not be awarded to a contractor in a third country or to a U.S. company with a limited FCL based on third-country ownership, control, or influence without the express written consent of the originating foreign government. The CSA will coordinate with the appropriate foreign government authorities.

Section 4. International Transfers

10-400. General. This section contains the procedures for international transfers of classified material. The requirements in this section do not apply to the transmission of classified material to U.S. Government activities outside the United States.

10-401. International Transfers of Classified Material

a. All international transfers of classified material shall take place through channels approved by both governments. Control of classified material must be maintained until the material is officially transferred to the intended recipient government through its designated government representative (DGR).

b. To ensure government control, written transmission instructions shall be prepared for all international transfers of classified material. Preparation of the instructions shall be the responsibility of the contractor for direct commercial arrangements, and the GCA for government arrangements.

c. The CSA shall be contacted at the earliest possible stage in deliberations that will lead to the international transfer of classified material. The CSA shall advise the contractor on the transfer arrangements, identify the recipient government's DGR, appoint a U.S. DGR, and ensure that the transportation plan prepared by the contractor or foreign government is adequate.

d. Requests for export authorizations that will involve the transfer of classified material shall be accompanied by a Department of State Form DSP-83, Non-Transfer and Use Certificate. The form shall be signed by an official of the responsible foreign government who has the authority to certify that the transfer is for government purposes and that the classified material will be protected in compliance with a government-approved security agreement.

10-402. Transfers of Freight

a. Transportation Plan (TP). A requirement to prepare a TP shall be included in each arrangement that involves the international transfer of classified material as freight. The TP shall describe arrangements for the secure shipment of the material from the point of origin to the ultimate destination. The U.S. and recipient government DGRs shall be identified in the TP as well as any requirement for an escort. The TP shall provide for security arrangements in the event the transfer cannot be made promptly. When there are to be repetitive shipments, a Notice of Classified Consignment will be used.

b. Government Agency Arrangements. Classified material to be furnished to a foreign government under such transactions normally will be shipped via government agency-arranged transportation and be transferred to the foreign government's DGR within the recipient government's territory. The government agency that executes the arrangement is responsible, in coordination with the recipient foreign government, for preparing a TP. When the point of origin is a U.S. contractor facility, the GCA shall provide the contractor a copy of the TP and the applicable Letter of Offer and Acceptance (LOA). If a freight forwarder is to be used in processing the shipment, the freight forwarder shall be provided a copy of the TP by the GCA.

c. Commercial Arrangements. The contractor shall prepare a TP in coordination with the receiving government. This requirement applies whether the material is to be moved by land, sea, or air, and applies to U.S. and foreign classified contracts. After the CSA approves the TP, it shall be forwarded to the recipient foreign government security authorities for final coordination and approval.

d. International Carriers. The international transfer of classified material shall be made using only ships, aircraft, or other carriers that:

(1) Are owned or chartered by the U.S Government or under U.S. registry,

(2) Are owned or chartered by or under the registry of the recipient government, or

(3) Are carriers other than those described that are expressly authorized to perform this function in writing by the Designated Security Authority of the GCA and the security authorities of the foreign government involved. This authority shall not be delegated and this exception may be authorized only when a carrier described in (1) or (2) above is not available and/or an urgent operational requirement dictates use of the exception.

10-403. Return of Material for Repair, Modification, or Maintenance. A foreign government or contractor may return classified material to a U.S. contractor for repair, modification, or maintenance. The approved methods of return shall be specified in either the GCA sales arrangement, the security requirements section of a direct commercial sales arrangement, or, in the case of material transferred as freight, in the original TP. The contractor, on receipt of notification that classified material is to be received, shall notify the applicable CSA.

10-404. Use of Freight Forwarders.

a. A commercial freight forwarder may be used to arrange for the international transfer of classified material as freight. The freight forwarder must be under contract to a government agency, U.S. contractor, or the recipient foreign government. The contract shall describe the specific functions to be performed by the freight forwarder. The responsibility for security and control of the classified material that is processed by freight forwarders remains with the U.S. Government until the freight is transferred to a DGR of the recipient government.

b. Only freight forwarders that have a valid FCL and storage capability at the appropriate level are eligible to take custody or possession of classified material for delivery as freight to foreign recipients. Freight forwarders that only process unclassified paperwork and make arrangements for the delivery of classified material to foreign recipients do not require an FCL.

10-405. Handcarrying Classified Material. To meet contractual requirements, the CSA may authorize contractor employees to handcarry classified material outside the United States. SECRET is the highest level of classified material to be carried and it shall be of such size and weight that the courier can retain it in his or her possession at all times. The CSA shall ensure that the contractor has made necessary arrangements with U.S. airport security and customs officials and that security authorities of the receiving government approve the plan. If the transfer is under a contract or a bilateral or multinational government program, the request shall be approved in writing by the GCA. The CSA shall be notified by the contractor of a requirement under this section at least 5 work days in advance of the transfer. In addition:

a. The courier shall be a full-time, appropriately cleared employee of the dispatching contractor.

b. The courier shall be provided with a Courier Certificate that shall be consecutively numbered and be valid for one journey only. The journey may include more than one stop if approved by the CSA and secure Government storage has been arranged at each stop. The Courier Certificate shall be returned to the dispatching security officer immediately on completion of the journey.

c. Before commencement of each journey, the courier shall read and initial the Notes to the Courier attached to the Courier Certificate and sign the Courier Declaration. The Declaration shall be maintained by the FSO until completion of the next security inspection by the CSA.

d. The material shall be inventoried, and shall be wrapped and sealed in the presence of the U.S. DGR. The address of the receiving security office and the return address of the dispatching company security office shall be shown on the inner envelope or wrapping. The address of the receiving government's DGR shall be shown on the outer envelope or wrapping along with the return address of the dispatching office.

e. The dispatching company security office shall prepare three copies of a receipt based on the inventory and list the classified material involved. One copy of the receipt shall be retained by the dispatching company security office. The other two copies shall be packed with the classified material. The security office shall obtain a receipt for the sealed package from the courier.

f. The dispatching company security office shall provide the receiving security office with 24 work hours advance notification of the anticipated date and time of the courier's arrival and the identity of the courier. The receiving security office shall notify the dispatching company security office if the courier does not arrive within 8 hours of the expected time of arrival. The dispatching security office shall notify its DGR of any delay, unless officially notified otherwise of a change in the courier's itinerary.

g. The receiving DGR shall verify the contents of the consignment and shall sign the receipts enclosed in the consignment. One copy shall be returned to the courier. On return, the courier shall provide the executed receipt to the dispatching security office.

h. Throughout the journey, the consignment shall remain under the direct personal control of the courier. It shall not be left unattended at any time during the journey, in the transport being used, in hotel rooms, in

cloakrooms, or other such location, and it may not be deposited in hotel safes, luggage lockers, or in luggage offices. In addition, envelopes and packages containing the classified material shall not be opened en route, unless required by customs or other government officials.

i. When inspection by government officials is unavoidable, the courier shall request that the officials provide written verification that they have opened the package. The courier shall notify the FSO as soon as possible. The FSO shall notify the U.S. DGR. If the inspecting officials are not of the same country as the dispatching security office, the designated security authority in the country whose officials inspected the consignment shall be notified by the CSA. Under no circumstances shall the classified consignment be handed over to customs or other officials for their custody.

j. When carrying classified material, the courier shall not travel by surface routes through third countries, except as authorized by the CSA. The courier shall travel only on carriers described in 10-402d, and travel direct routes between the U.S. and the destination.

10-406. Classified Material Receipts. There shall be a continuous chain of receipts to record international transfers of all classified material from the contractor through the U.S. DGR and the recipient DGR to the ultimate foreign recipient. The contractor shall retain an active suspense record until return of applicable receipts for the material. A copy of the external receipt that records the passing of custody of the package containing the classified material shall be retained by the contractor and each intermediate consignee in a suspense file until the receipt that is enclosed in the package is signed and returned. Follow-up action shall be initiated through the CSA if the signed receipt is not returned within 45 days.

10-407. Contractor Preparations for International Transfers Pursuant to Commercial and User Agency Sales. The contractor shall be responsible for the following preparations to facilitate international transfers:

a. Ensure that each party to be involved in the transfer is identified in the applicable contract or agreement, and in the license application or letter request.

b. Notify the appropriate U.S. DGR when the material is ready.

c. Provide documentation or written certification by an empowered official (as defined in the ITAR) to the U.S. DGR to verify that the classified shipment is within the limitations of the pertinent export authorization or an authorized exemption to the export authorization requirements, or is within the limitations of the pertinent GCA contract.

d. Have the classified shipment ready for visual review and verification by the DGR. As a minimum this will include:

(1) Preparing the packaging materials, address labels, and receipts for review.

(2) Marking the contents with the appropriate U.S. classification or the equivalent foreign government classification, downgrading, and declassification markings, as applicable.

(3) Ensuring that shipping documents (including, as appropriate, the Shipper's Export Declaration) include the name and contact information for the CSA that validates the license or letter authorization, and the FSO or designee for the particular transfer.

(4) Sending advance notification of the shipment to the CSA, the recipient, and to the freight forwarder, if applicable. The notification will require that the recipient confirm receipt of the shipment or provide notice to the contractor if the shipment is not received in accordance with the prescribed shipping schedule.

10-408. Transfers of Technical Data Pursuant to an ITAR Exemption

a. The contractor shall provide to the DGR valid documentation (i.e., license, Letter of Offer and Acceptance, or agreement) to verify the export authorization for classified technical data to be transferred under an exemption to reference (w). The documentation shall include a copy of the Form DSP-83 associated with the original export authorization.

b. Classified technical data to be exported pursuant to reference (w) exemptions 125.4(b)(1), 125.4(c), 125.5, 126.4(a), or 126.4(c) shall be supported by a written authorization signed by an Authorized Exemption Official or Exemption Certifying Official who has been appointed by the responsible Principal Disclosure Authority of the GCA. A copy of the authorization shall be provided by the contractor through the CSA to the Office of Defense Trade Controls.

c. Exports shall not be permitted under a Manufacturing License or Technical Assistance Agreement for which the authorization has expired.

Section 5. International Visits and Control of Foreign Nationals

10-500. General. This section describes the procedures that the United States and foreign governments have established to control international visits to their organizations and cleared contractor facilities.

10-501. International Visits

a. The contractor shall establish procedures to monitor international visits by their employees and visits or assignments to their facilities of foreign nationals to ensure that the disclosure of, and access to, export-controlled articles and related information are limited to those that are approved by an export authorization.

b. Visit authorizations shall not be used to employ or otherwise acquire the services of foreign nationals that require access to export-controlled information. An export authorization is required for such situations.

10-502. Types and Purpose of International Visits. Visit requests are necessary to make administrative arrangements and disclosure decisions, and obtain security assurances. There are three types of international visits:

a. **One-time Visits.** A visit for a single, short-term occasion (normally less than 30 days) for a specified purpose.

b. **Recurring Visits.** Intermittent, recurring visits over a specified period of time, normally up to 1 year in duration, in support of a Government-approved arrangement, such as an agreement, contract, or license. By agreement of the governments, the term of the authorization may be for the duration of the arrangement, subject to annual review, and validation.

c. **Extended Visits.** A single visit for an extended period of time, normally up to 1 year, in support of an agreement, contract, or license.

10-503. Emergency Visits. Some foreign governments will accept a visit request submitted within 7 calendar days of the proposed visit for an "emergency visit." To qualify as an emergency visit, the visit must relate to a specific Government-approved contract, international agreement or announced request for proposal, and failure to make the visit could be reasonably expected to seriously jeopardize performance on the contract or program, or result in the loss of a contract opportunity. Emergency visits are approved only as a single, one-time visit. The requester should coordinate the emergency visit in advance with the person to be visited and ensure that the complete name, position, address, and telephone number of the person and a knowledgeable foreign government point of contact are provided in the visit request, along with the identification of the contract, agreement, or program and the justification for submission of the emergency visit request.

10-504. Requests for Recurring Visits. Recurring visit authorizations should be requested at the beginning of each program. After approval of the request, individual visits may be arranged directly with the security office of the location to be visited subject to 3 working days advance notice.

10-505. Amendments. Visit requests that have been approved or are being processed may be amended only to change, add, or delete names and change dates. Amendments requesting earlier dates than originally specified shall not be accepted. Emergency visit authorizations shall not be amended.

10-506. Visits Abroad by U.S. Contractors. Many foreign governments require the submission of a visit request for all visits to a government facility or a cleared contractor facility, even though classified information may not be involved. They also require that the requests be received a specified number of days in advance of the visit. These lead times for North Atlantic Treaty Organization (NATO) countries are in Appendix B. An export authorization must be obtained if export controlled technical data is to be disclosed or, if information to be divulged is related to a classified U.S. Government program, unless the disclosure of the information is covered by an ITAR exemption. Visit request procedures are outlined as follows:

a. Request Format. The visit request format is contained in Appendix B. The visit request shall be forwarded to the security official designated by the CSA. The host for the visit should coordinate the visit in advance with appropriate government authorities who are required to approve the visit. It is the visitor's responsibility to ensure that such coordination has occurred.

b. Government Agency Programs. When contractor employees are to visit foreign government

facilities or foreign contractors on U.S. Government orders in support of a government contract or agreement, a visit request shall be submitted by the contractor.

10-507. Visits by Foreign Nationals to U.S. Contractor Facilities. Requests for visits by foreign nationals to U.S. contractor facilities that will involve the disclosure of (a) classified information, (b) unclassified information related to a U.S. Government classified program, or (c) plant visits covered by Section 125.5 of reference (w) shall be processed through the sponsoring foreign government (normally the visitor's embassy) to the U.S. Government agency for approval. (NOTE: Requests for visits by foreign nationals that involve only commercial programs and related unclassified information may be submitted directly to the contractor. It is the contractor's responsibility to ensure that an export authorization is obtained, if applicable.) As described below, the U.S. government agency may approve or deny the request or decline to render a decision.

a. **Government-Approved Visits.** U.S. Government-approved visits constitute an exemption to the export licensing provisions of the ITAR. U.S. Government approved visits shall not be used to avoid the export licensing requirements for commercial initiatives. When the cognizant U.S. Government agency approves a visit, the notification of approval shall contain instructions on the level and scope of classified and unclassified information authorized for disclosure, as well as any limitations. Final acceptance of the visit shall be subject to the concurrence of the contractor who shall notify the U.S. Government agency when a visit is not desired.

b. **Visit Request Denials.** If the U.S. Government agency does not approve the disclosure of the information related to the proposed visit, it will deny the visit request. The requesting government and the contractor to be visited shall be advised of the reason for the denial. The contractor may accept the visitor(s). However, only information that is in the public domain may be disclosed.

c. **Non-Sponsorship.** The U.S. Government agency will decline to render a decision on a visit request that is not in support of a U.S. Government program. A declination notice indicating that the visit is not government-approved (i.e., the visit is non-sponsored) shall be furnished to the requesting foreign government with an information copy to the U.S. contractor to be visited. A declination notice does not preclude the visit, provided the contractor has, or obtains, an export authorization for the information involved and, if classified information is involved, has been notified that the requesting foreign government has provided the required security assurance of the proposed visitor to the U.S. Government agency in the original visit request. It shall be the responsibility of the contractor to consult applicable export regulations to determine licensing requirements regarding the disclosure of export controlled information during such visits by foreign nationals.

d. **Access by Foreign Visitors to Classified Information.** The contractor shall establish procedures to ensure that foreign visitors are not afforded access to classified information and other export-controlled technical data except as authorized by an export license, approved visit request, or other exemption to the licensing requirements. The contractor shall not inform the foreign visitor of the scope of access authorized or of the limitations imposed by the government. Foreign visitors shall not be given custody of classified material except when they are acting as official couriers of their government and the CSA authorizes the transfer.

e. **Visitor Records**. The contractor shall maintain a record of foreign visitors when the visit involves access to classified information. These records shall be maintained for 1 year.

f. **Visits to Subsidiaries.** A visit request authorization for a visit to any element of a corporate family may be used for visits to other divisions or subsidiaries within the same corporate family provided disclosures are for the same purpose and the information to be disclosed does not exceed the parameters of the approved visit request.

10-508. Control of Access by On-Site Foreign Nationals

a. Extended visits and assignments of foreign nationals to contractor facilities shall be authorized only when it is essential that the foreign national be at the facility pursuant to a contract or government agreement (e.g., joint venture, liaison representative to a joint or multinational program, or direct commercial sale).

b. If the foreign national will require access to export-controlled information related to, or derived from, a U.S. Government classified contract, the contractor shall obtain the written consent of the GCA before making a commitment to accept the proposed visit or assignment. A copy of the written consent shall be included with the request for export authorization, when such authorization is required.

c. The applicable CSA shall be notified in advance of all extended visits and assignments of foreign nationals to cleared contractor facilities. The notification shall include a copy of the approved visit authorization or the U.S. Government export authorization, and the TCP if applicable.

d. Classified U.S. and foreign government material in a U.S. contractor facility is to remain under U.S. contractor custody and control and is subject to inspection by the FSO and the CSA. This does not preclude a foreign visitor from being furnished a security container for the temporary storage of classified material, consistent with the purpose of the visit or assignment, provided the CSA approves and responsibility for the container and its contents remains with the U.S. contractor. Exceptions to this policy may be approved on a case-by-case basis by the CSA for the storage of foreign government classified information furnished to the visitor by the visitor's government through government channels. Exceptions shall be approved in advance in writing by the CSA and agreed to by the visitor's government. The agreed procedures shall be included in the contractor's TCP, shall require the foreign nationals to provide receipts for the material, and shall include an arrangement for the CSA to ensure compliance, including provisions for the CSA to inspect and inventory the material.

10-509. TCP. A TCP is required to control access by foreign nationals assigned to, or employed by, cleared contractor facilities unless the CSA determines that procedures already in place at the contractor's facility are adequate. The TCP shall contain procedures to control access for all export-controlled information. A sample of a TCP may be obtained from the CSA.

10-510. Security and Export Control Violations Involving Foreign Nationals. Any violation of administrative security procedures or export control regulations that would subject classified information to possible compromise by foreign visitors or foreign national employees shall be reported to the CSA.

Section 6. Contractor Operations Abroad

10-600. General. This section sets forth requirements governing contractor operations abroad, including PCLs for U.S. contractor employees assigned outside the United States and their access to classified information.

10-601. Access by Contractor Employees Assigned Outside the United States.

a. Contractor employees assigned outside the United States, its possessions or territories may have access to classified information in connection with performance on a specified United States, NATO, or foreign government classified contract.

b. The assignment of an employee who is a foreign national, including intending citizens, outside the United States on programs that will involve access to classified information is prohibited and negates the basis on which an LAA may have been provided to such employee.

c. A consultant shall not be assigned outside the United States with responsibilities requiring access to classified information.

10-602. Storage, Custody, and Control of Classified Information Abroad by Employees of a U.S. Contractor.

a. The storage, custody, and control of classified information required by a U.S. contractor employee abroad is the responsibility of the U.S. Government. Therefore, the storage of classified information by contractor employees at any location abroad that is not under U.S. Government control is prohibited. The storage may be at a U.S. military facility, a U.S. Embassy or Consulate, or other location occupied by a U.S. Government organization.

b. A contractor employee may be furnished a security container to temporarily store classified material at a U.S. Government agency overseas location. The decision to permit a contractor to temporarily store classified information must be approved in writing by the senior security official for the U.S. Government host organization.

c. A contractor employee may be permitted to temporarily remove classified information from an overseas U.S. Government-controlled facility when necessary for the performance of a GCA contract or pursuant to an approved export authorization. The responsible U.S. Government security official at the U.S. Government facility shall verify that the contractor has an export authorization or other written U.S. Government approval to have the material, verify the need for the material to be removed from the facility, and brief the employee on handling procedures. In such cases, the contractor employee shall sign a receipt for the classified material. Arrangements shall also be made with the U.S. Government custodian for the return and storage of the classified material during non-duty hours. Violations of this policy shall be reported to the applicable CSA by the security office at the U.S. Government facility.

d. A contractor employee shall not store classified information at overseas divisions or subsidiaries of U.S. companies incorporated or located in a foreign country. (NOTE: The divisions or subsidiaries may possess classified information that has been transferred to the applicable foreign government through government-to-government channels pursuant to an approved export authorization or other written U.S. Government authorization. Access to this classified information at such locations by a U.S. contractor employee assigned abroad by the parent facility on a visit authorization in support of a foreign government contract or subcontract, is governed by the laws and regulations of the country in which the division or subsidiary is registered or incorporated. The division or subsidiary that has obtained the information from the foreign government shall provide the access.)

e. U.S. contractor employees assigned to foreign government or foreign contractor facilities under a direct commercial sales arrangement will be subject to the host-nation's industrial security policies.

10-603. Transmission of Classified Material to Employees Abroad. The transmission of classified material to a cleared contractor employee located outside the United States shall be through U.S. Government channels. If the material is to be used for other than U.S. Government purposes, an export authorization is required and a copy of the authorization, validated by the DGR, shall accompany the material. The material shall be addressed to a U.S. military organization or other U.S. Government organization (e.g., an embassy). The U.S. government organization abroad shall be responsible for custody and control of the material.

10-604. Security Briefings. An employee being assigned outside the United States shall be briefed on the security requirements of his or her assignment, including the handling, disclosure, and storage of classified information overseas.

Section 7. NATO Information Security Requirements

10-700. General. This section provides the security requirements needed to comply with the procedures established by the U.S. Security Authority for NATO (USSAN) for safeguarding NATO information provided to U.S. industry.

10-701. Classification Levels. NATO has the following levels of security classification: COSMIC TOP SECRET (CTS), NATO SECRET (NS), NATO CONFIDENTIAL (NC), and NATO RESTRICTED (NR). Another marking, ATOMAL, is applied to U.S. RESTRICTED DATA or FORMERLY RESTRICTED DATA and United Kingdom Atomic information that has been released to NATO. ATOMAL information is marked COSMIC TOP SECRET ATOMAL (CTSA), NATO SECRET ATOMAL (NSA), or NATO CONFIDENTIAL ATOMAL (NCA).

10-702. NATO RESTRICTED. NATO RESTRICTED does not correspond to an equivalent U.S. classification. NATO RESTRICTED does not require a PCL for access. An FCL is not required if the only information to which the company will have access is NATO RESTRICTED. IS handling only NATO RESTRICTED information do not require certification or accreditation. NATO RESTRICTED information may be included in U.S. unclassified documents. The U.S. document must be marked, "THIS DOCUMENT CONTAINS NATO RESTRICTED INFORMATION." NATO RESTRICTED material may be stored in locked filing cabinets, bookcases, desks, or other similar locked containers that will deter unauthorized access.

10-703. NATO Contracts. NATO contracts involving NATO-unique systems, programs, or operations are awarded by a NATO Production and Logistics Organization (NPLO), a designated NATO Management Agency, the NATO Research Staff, or a NATO Command. In the case of NATO infrastructure projects (e.g., airfields, communications), the NATO contract is awarded by a contracting agency or prime contractor of the NATO nation responsible for the infrastructure project.

10-704. NATO Facility Security Clearance Certificate. A NATO Facility Security Clearance Certificate (FSCC) is required for a contractor to negotiate or perform on a NATO classified contract A U.S. facility qualifies for a NATO FSCC if it has an equivalent U.S. FCL and its personnel have been briefed on NATO procedures. The CSA shall provide the NATO FSCC to the requesting activity. A NATO FSCC is not required for GCA contracts involving access to NATO classified information.

10-705. PCL Requirements. Access to NATO classified information requires a final PCL at the equivalent level.

10-706. NATO Briefings. Before having access to NATO classified information, employees shall be given a NATO security briefing that covers the requirements of this section and the consequences of negligent handling of NATO classified information. The FSO shall be initially briefed by a representative of the CSA. Annual refresher briefings shall also be conducted. When access to NATO classified information is no longer required, the employee shall be debriefed. The employee shall sign a certificate stating that they have been briefed or debriefed, as applicable, and acknowledge their responsibility for safeguarding NATO information. Certificates shall be maintained for 2 years for NATO SECRET and CONFIDENTIAL, and 3 years for COSMIC TOP SECRET and all ATOMAL information. The contractor shall maintain a record of all NATO briefings and debriefings in the CSA-designated database.

10-707. Access to NATO Classified Information by Foreign Nationals. Foreign nationals of non-NATO nations may have access to NATO classified information only with the consent of the NATO Office of Security and the contracting activity. Requests shall be submitted to the Central U.S. Registry (CUSR). Access to NATO classified information may be permitted for citizens of NATO member nations, provided a NATO security clearance certificate is provided by their government and they have been briefed.

10-708. Subcontracting for NATO Contracts. The contractor shall obtain prior written approval from the NATO contracting activity and a NATO FSCC must be issued prior to awarding the subcontract. The request for approval will be forwarded through the CSA.

10-709. Preparing and Marking NATO Documents. All classified documents created by a U.S. contractor shall be portion-marked. Any portion extracted from a NATO document that is not portion

marked, must be assigned the classification that is assigned to the NATO document.

a. All U.S.-originated NATO classified documents shall bear an assigned reference number and date on the first page. The reference numbers shall be assigned as follows:

(1) The first element shall be the abbreviation for the name of the contractor facility.

(2) The second element shall be the abbreviation for the overall classification followed by a hyphen and the 4-digit sequence number for the document within that classification that has been generated for the applicable calendar year.

(3) The third element shall be the year; e.g., MM/NS-0013/93.

b. COSMIC TOP SECRET, NATO SECRET, and ATOMAL documents shall bear the reference number on each page and a copy number on the cover or first page. Copies of NATO documents shall be serially numbered. Pages shall be numbered. The first page or index or table of contents shall include a list, including page numbers, of all Annexes and Appendices. The total number of pages shall be stated on the first page. All Annexes or Appendices will include the date of the original document and the purpose of the new text (addition or substitution) on the first page.

c. One of the following markings shall be applied to NATO documents that contain ATOMAL information:

(1) "This document contains U.S. ATOMIC Information (RESTRICTED DATA or FORMERLY RESTRICTED DATA) made available pursuant to the NATO Agreement for Cooperation Regarding ATOMIC Information, dated 18 June 1964, and will be safeguarded accordingly."

(2) "This document contains UK ATOMIC Information. This information is released to NATO including its military and civilian agencies and member states on condition that it will not be released by the recipient organization to any other organization or government or national of another country or member of any other organization without prior permission from H.M. Government in the United Kingdom."

d. Working papers shall be retained only until a final product is produced.

10-710. Classification Guidance. Classification guidance shall be in the form of a NATO security aspects letter and a security requirements checklist for NATO contracts, or a Contract Security Classification Specification. If adequate classification guidance is not received, the contractor shall contact the CSA for assistance. NATO classified documents and NATO information in other documents shall not be declassified or downgraded without the prior written consent of the originating activity. Recommendations concerning the declassification or downgrading of NATO classified information shall be forwarded to the CUSR.

10-711. Further Distribution. The contractor shall not release or disclose NATO classified information to a third party or outside the contractor's facility for any purpose without the prior written approval of the contracting agency.

10-712. Storage of NATO Documents. NATO classified documents shall be stored as prescribed for U.S. documents of an equivalent classification level, except as follows:

a. NATO classified documents shall not be commingled with other documents.

b. Combinations for containers used to store NATO classified information shall be changed annually. The combination also shall be changed when an individual with access to the container departs or no longer requires access to the container, and if the combination is suspected of being compromised.

c. When the combination is recorded it shall be marked with the highest classification level of documents stored in the container as well as to indicate the level and type of NATO documents in the container. The combination record must be logged and controlled in the same manner as NATO classified documents.

10-713. International Transmission. NATO has a registry system for the receipt and distribution of NATO documents within each NATO member nation. The central distribution point for the U.S. is the CUSR located in the Pentagon. The CUSR establishes subregistries at U.S. Government organizations for further distribution and control of NATO documents. Subregistries may establish control points at contractor facilities. COSMIC TOP SECRET, NATO SECRET, and all ATOMAL documents shall be transferred through the registry system. NATO CONFIDENTIAL documents provided as part of NATO infrastructure

contracts shall be transmitted via government channels in compliance with Section 4 of this Chapter.

10-714. Handcarrying. NATO SECRET and NATO CONFIDENTIAL documents may be handcarried across international borders if authorized by the GCA. The courier shall be issued a NATO Courier Certificate by the CSA. When handcarrying is authorized, the documents shall be delivered to a U.S. organization at NATO, which shall transfer them to the intended NATO recipient.

10-715. Reproduction. Reproductions of COSMIC TOP SECRET and COSMIC TOP SECRET ATOMAL information shall be performed by the responsible Registry. The reproduction of NATO SECRET, and CONFIDENTIAL documents may be authorized to meet contractual requirements unless reproduction is prohibited by the contracting entity. Copies of COSMIC TOP SECRET, NATO SECRET, and ATOMAL documents shall be serially numbered and controlled and accounted for in the same manner as the original.

10-716. Disposition. Generally, all NATO classified documents shall be returned to the contracting activity that provided them on completion of the contract. Documents provided in connection with an invitation to bid also shall be returned immediately if the bid is not accepted or submitted. NATO classified documents may also be destroyed when permitted. COSMIC TOP SECRET and COSMIC TOP SECRET ATOMAL documents shall be destroyed by the Registry that provided the documents. Destruction certificates are required for all NATO classified documents except NATO CONFIDENTIAL. The destruction of COSMIC TOP SECRET, NATO SECRET and all ATOMAL documents must be witnessed.

10-717. Accountability Records. Logs, receipts, and destruction certificates are required for NATO classified information, as described below. Records for NATO documents shall be maintained separately from records of non-NATO documents. COSMIC TOP SECRET and all ATOMAL documents shall be recorded on logs maintained separately from other NATO logs and shall be assigned unique serial control numbers. Additionally, disclosure records bearing the name and signature of each person who has access are required for all COSMIC TOP SECRET, COSMIC TOP SECRET ATOMAL, and all other ATOMAL or NATO classified documents to which special access limitations have been applied.

a. Minimum identifying data on logs, receipts, and destruction certificates shall include the NATO reference number, short title, date of the document, classification, and serial copy numbers. Logs shall reflect the short title, unclassified subject, and distribution of the documents.

b. Receipts are required for all NATO classified documents except NATO CONFIDENTIAL.

c. Inventories shall be conducted annually of all COSMIC TOP SECRET, NATO SECRET, and all ATOMAL documents.

d. Records shall be retained for 10 years for COSMIC TOP SECRET and COSMIC TOP SECRET ATOMAL documents and 5 years for NATO SECRET, NATO SECRET ATOMAL, NATO CONFIDENTIAL, and NATO CONFIDENTIAL ATOMAL documents.

10-718. Security Violations and Loss, Compromise, or Possible Compromise. The contractor shall immediately report the loss, compromise, or suspected loss or compromise, as well as any other security violations involving NATO classified information to the CSA.

10-719. Extracting from NATO Documents. Permission to extract from a COSMIC TOP SECRET or ATOMAL document shall be obtained from the CUSR.

a. If extracts of NATO information are included in a U.S. document prepared for a non-NATO contract, the document shall be marked with U.S. classification markings. The caveat, "THIS DOCUMENT CONTAINS NATO (level of classification) INFORMATION" also shall be marked on the front cover or first page of the document. Additionally, each paragraph or portion containing the NATO information shall be marked with the appropriate NATO classification, abbreviated in parentheses (e.g., NS) preceding the portion or paragraph. The "Declassify on" line of the document shall show "Source marked OADR" and the date of origin of the most recent source document unless the original NATO document shows a specific date for declassification.

b. The declassification or downgrading of NATO information in a U.S. document requires the approval of the originating NATO activity. Requests shall be submitted to the CUSR for NATO contracts, through the GCA for U.S. contracts, and through the CSA for non-NATO contracts awarded by a NATO member nation.

10-720. Release of U.S. Information to NATO.

a. Release of U.S. classified or export-controlled information to NATO requires an export authorization or other written disclosure authorization. When a document containing U.S. classified information is being prepared for NATO, the appropriate NATO classification markings shall be applied to the document. Documents containing U.S. classified information and U.S. classified documents that are authorized for release to NATO shall be marked on the cover or first page "THIS DOCUMENT CONTAINS U.S. CLASSIFIED INFORMATION. THE INFORMATION IN THIS DOCUMENT HAS BEEN AUTHORIZED FOR RELEASE TO (cite the NATO organization) BY (cite the applicable license or other written authority)." The CSA shall provide transmission instructions to the contractor. The material shall be addressed to a U.S. organization at NATO, which shall then place the material into NATO security channels. The material shall be accompanied by a letter to the U.S. organization that provides transfer instructions and assurances that the material has been authorized for release to NATO. The inner wrapper shall be addressed to the intended NATO recipient. Material to be sent to NATO via mail shall be routed through the U.S. Postal Service and U.S. military postal channels to the U.S. organization that will make the transfer.

b. A record shall be maintained that identifies the originator and source of classified information that are used in the preparation of documents for release to NATO. The record shall be provided with any request for release authorization.

10-721. Visits. NATO visits are visits by personnel representing a NATO entity and relating to NATO contracts and programs. NATO visits shall be handled in accordance with the requirements in Section 5 of this chapter. A NATO Certificate of Security Clearance will be included with the visit request.

a. NPLO and NATO Industrial Advisory Group (NIAG) Recurring Visits. NATO has established special procedures for recurring visits involving contractors, government departments and agencies, and NATO commands and agencies that are participating in a NPLO or NIAG contract or program. The NATO Management Office or Agency responsible for the NPLO program will prepare a list of the Government and contractor facilities participating in the program. For NIAG programs, the list will be prepared by the responsible NATO staff element. The list will be forwarded to the appropriate clearance agency of the participating nations, which will forward it to the participating contractor.

b. **Visitor Record.** The contractor shall maintain a record of NATO visits including those by U.S. personnel assigned to NATO. The records shall be maintained for 3 years.

CHAPTER 11
Miscellaneous Information

Section 1. TEMPEST

11-100. General. TEMPEST is an unclassified short name referring to investigations and studies of compromising emanations. Compromising emanations are unintentional intelligence-bearing signals that, if intercepted and analyzed, will disclose classified information when it is transmitted, received, handled, or otherwise processed by any information processing equipment.

11-101. TEMPEST Requirements.

a. TEMPEST countermeasures will be applied only in proportion to the threat of exploitation and the resulting damage to the national security should the information be intercepted and analyzed by a foreign intelligence organization. It is the responsibility of the GCA to identify in writing what TEMPEST countermeasures may be required. The GCA will identify any TEMPEST requirements within the United States to the CSA for approval prior to imposing requirements for TEMPEST countermeasures on contractors. Contractors may not impose TEMPEST countermeasures upon their subcontractors without GCA and CSA approval.

b. The government is responsible for performing threat assessment and vulnerability studies when it is determined that classified information may be exposed to TEMPEST collection.

c. Contractors will assist the GCA in conducting threat and vulnerability surveys by providing the following information upon request:

(1) The specific classification and special categories of material to be processed/handled by electronic means.

(2) The specific location where classified processing will be performed.

(3) The name, address, title, and contact information for a point-of-contact at the facility where processing will occur.

11-102. Cost. All costs associated with applying TEMPEST countermeasures, when such countermeasures are imposed upon the contractor by a GCA, shall be recoverable by direct charge to the applicable contract. The GCA should provide TEMPEST shielding and shielded equipments as government-furnished equipment (GFE) when such extreme countermeasures are deemed essential to the protection of the information being processed.

Section 2. Defense Technical Information Center (DTIC)

11-200. General. The Department of Defense operates certain activities to assist individuals and organizations in gaining access to scientific and technical information describing planned or on-going research, development, technical and engineering (RDT&E) efforts of the Department of Defense. DTIC is the central point within the Department of Defense for acquiring, storing, retrieving, and disseminating scientific and technical information to support the management and conduct of DoD RDT&E and study programs.

11-201. User Community. DTIC services are available to the Department of Defense and its contractors, as well as to other U.S. Government organizations and their contractors. Contractors may also become eligible for services under the Defense Potential Contractors Program.

11-202. Registration Process. All users are required to register for service. Registration, which is free, generally involves completing two forms which are available from DTIC as part of a registration kit.

a. DD Form 1540, Registration for Scientific and Technical Information Services. This form shall be completed for each contract that authorizes use of DTIC services. This authorization is included in the Contract Security Classification Specification. The DD Form 1540 is submitted to DTIC through the sponsoring GCA for certification and approval. If a subcontract is involved, the DD Form 1540 is submitted through the prime contractor. The DD Form 1540 remains in force until completion of the classified contract or subcontract.

b. DD Form 2345, Militarily Critical Technical Data Agreement. Qualified contractors are eligible for access to militarily critical technical data after certification with Defense Logistics Services Center (DLSC) by completing the DD Form 2345. This DLSC certification is supplementary to registration with the DTIC. Upon certification with DLSC, the user also may be eligible for access to unclassified, militarily critical technical data from other DoD sources.

11-203. Safeguarding Requirements. Classified information acquired from DTIC shall be safeguarded according to the requirements of this Manual and with any restrictions that are marked on the material itself. The specific contract number that authorized contractor access to the information shall be placed on each classified document. When the contract to which the DD Form 1540 applies is completed or terminated, the contractor shall either destroy or request retention for the material.

11-204. DTIC Downgrading or Declassification Notices. DTIC re-marks downgraded or declassified paper documents only on the front and back covers and the title, first, and back pages. It is the responsibility of the recipient to complete any remarking required. Documents originally marked under the provisions of previous E.O.s may contain pages that do not bear any classification markings. Before extracting or reproducing the information from these pages, contractors should direct any questions they may have to the originator of the document.

11-205. Questions Concerning Reference Material. Most material made available to contractors by DTIC and other distribution agencies is reference material. Therefore, the GCA that authorized the services of DTIC under a specific contract may not be in a position to provide the contractor with classification guidance for the reference material. Classification jurisdiction always is the responsibility of the originating agency, or its successor. Classification jurisdiction is not necessarily the responsibility of the authorizing GCA. When a contractor needs assistance in identifying the responsible department or agency for classification guidance for reference material the CSA should be consulted.

11-206. Subcontracts. If a contractor awards a subcontract that authorizes the subcontractor to use the services of DTIC and is expected to require access only to classified reference material, the Contract Security Classification Specification issued to the subcontractor shall show the highest category of classification required. The Contract Security Classification Specification will have a statement similar to the following: "Information extracted from classified reference material shall be classified according to the markings on such material. The DD Form 1540 prepared under this subcontract shall be forwarded through (name of prime contractor)."

Section 3. Independent Research and Development (IR&D) Efforts

11-300. General. This section provides special procedures and requirements necessary for safeguarding classified information when it is incorporated in contractors' IR&D efforts.

11-301. Information Generated Under an IR&D Effort that Incorporates Classified Information. Under reference (b) information that is in substance the same as information currently classified requires a derivative classification. Therefore, information in a contractor's IR&D effort will require a derivative classification.

11-302. Classification Guidance. The releasing contractor may extract guidance appropriate for the IR&D effort from:

a. An existing Contract Security Classification Specification that was previously furnished by a GCA in connection with performance of a classified contract;

b. A final Contract Security Classification Specification that was issued in connection with retention of classified documents under a completed contract;

c. A security classification guide obtained from DTIC; or

d. A classified source document.

NOTE: The Department of Defense "Index of Security Classification Guides" and many of the listed security classification guides are available to contractors who are registered with the DTIC. Contractors are encouraged to use the Index and the listed guides to obtain up-to-date security guidance for the classified information involved when developing guidance appropriate for their IR&D efforts.

11-303. Preparation of Security Guidance. Contractors shall use the Contract Security Classification Specification to provide security guidance for the classified information released in their IR&D efforts.

11-304. Retention of Classified Documents Generated Under IR&D Efforts. Contractors may retain the classified documents that were generated in connection with their classified IR&D efforts for the duration of their FCL provided they have proper storage capability. Documents shall be clearly identified as "IR&D DOCUMENTS." A contractor's facility clearance will not be continued solely for the purpose of retention of classified IR&D documents without specific retention authorization from the GCA that has jurisdiction over the classified information contained in such documents. Contractors shall establish procedures for review of their IR&D documents on a recurring basis to reduce their classified inventory to the minimum necessary