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 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 (f)).

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 expressly authorized 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 Tagli 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.

I-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.